Conselho da
União Europeia

Bruxelas, 6 de dezembro de 2022
(OR. en)

15698/22

Dossiê interinstitucional:
2021/0106(COD)

TELECOM 516
JAI 1633
COPEN 434
CYBER 399
DATAPROTECT 351
EJUSTICE 95
COSI 318
IXIM 291
ENFOPOL 626
RELEX 1674
MI 918
COMPET 1005
CODEC 1940

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	6 de dezembro de 2022
para:	Delegações
n.º doc. ant.:	14954/22 + ADD 1
n.° doc. Com.:	8115/21
Assunto:	Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União – Orientação geral (6 de dezembro de 2022)

Junto se envia, à atenção das delegações, a orientação geral do Conselho sobre a proposta em epígrafe, aprovada pelo Conselho (Transportes, Telecomunicações e Energia) na sua 3917.ª reunião, realizada em 6 de dezembro de 2022.

A orientação geral estabelece a posição provisória do Conselho sobre a presente proposta e constitui a base para a preparação das negociações com o Parlamento Europeu.

ANEXO

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

QUE ESTABELECE REGRAS HARMONIZADAS EM MATÉRIA DE INTELIGÊNCIA ARTIFICIAL (REGULAMENTO INTELIGÊNCIA ARTIFICIAL) E ALTERA DETERMINADOS ATOS LEGISLATIVOS DA UNIÃO

(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente os artigos 16.º e 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu[1],

Tendo em conta o parecer do Comité das Regiões[2],

Tendo em conta o parecer do Banco Central Europeu[3],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

---

1 JO C […] de […], p. […].
2 JO C […] de […], p. […].
3 Inserir referência ao parecer do BCE.

(1) A finalidade do presente regulamento é melhorar o funcionamento do mercado interno mediante o estabelecimento de um quadro jurídico uniforme para o desenvolvimento, a comercialização e a utilização da inteligência artificial em conformidade com os valores da União. O presente regulamento observa um conjunto de razões imperativas de reconhecido interesse público, como o elevado nível de proteção da saúde, da segurança e dos direitos fundamentais, e assegura a livre circulação transfronteiras de produtos e serviços baseados em inteligência artificial, evitando assim que os Estados-Membros imponham restrições ao desenvolvimento, à comercialização e à utilização dos sistemas de inteligência artificial, salvo se explicitamente autorizado pelo presente regulamento.

(2) Os sistemas de inteligência artificial (sistemas de IA) podem ser implantados facilmente em vários setores da economia e da sociedade, incluindo além fronteiras, e circular por toda a União. Certos Estados-Membros já ponderaram a adoção de regras nacionais para assegurar que a inteligência artificial seja segura e seja desenvolvida e utilizada em conformidade com as obrigações de proteção dos direitos fundamentais. As diferenças entre regras nacionais podem conduzir à fragmentação do mercado interno e reduzir a segurança jurídica para os operadores que desenvolvem, importam ou utilizam sistemas de IA. Como tal, é necessário assegurar um nível de proteção elevado e coerente em toda a União e evitar divergências que prejudiquem a livre circulação dos sistemas de IA e dos produtos e serviços conexos no mercado interno, mediante o estabelecimento de obrigações uniformes para os operadores e a garantia da proteção uniforme das razões imperativas de reconhecido interesse público e dos direitos das pessoas em todo o mercado interno, com base no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE). Visto que o presente regulamento contém regras específicas aplicáveis à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, nomeadamente restrições à utilização de sistemas de IA para a identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública, é apropriado basear este regulamento no artigo 16.º do TFUE, no respeitante a essas regras específicas. Face a essas regras específicas e ao recurso ao artigo 16.º do TFUE, é apropriado consultar o Comité Europeu para a Proteção de Dados.

(3) A inteligência artificial é uma família de tecnologias em rápida evolução, capaz de oferecer um vasto conjunto de benefícios económicos e sociais a todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a repartição de recursos e personalizar as soluções digitais disponibilizadas às pessoas e às organizações, a utilização da inteligência artificial pode conferir importantes vantagens competitivas às empresas e contribuir para progressos sociais e ambientais, por exemplo, nos cuidados de saúde, na agricultura, na educação e na formação, na gestão das infraestruturas, na energia, nos transportes e logística, nos serviços públicos, na segurança, na justiça, na eficiência energética e dos recursos e na atenuação das alterações climáticas e adaptação às mesmas.

(4) Ao mesmo tempo, em função das circunstâncias relativas à sua aplicação e utilização específicas, a inteligência artificial pode criar riscos e prejudicar interesses públicos e direitos protegidos pela legislação da União. Esses prejuízos podem ser materiais ou imateriais.

(5) Como tal, é necessário adotar um quadro jurídico da União que estabeleça regras harmonizadas em matéria de inteligência artificial para promover o desenvolvimento, a utilização e a adoção da inteligência artificial no mercado interno e que, ao mesmo tempo, proporcione um nível elevado de proteção de interesses públicos, como a saúde e a segurança e a proteção dos direitos fundamentais, conforme reconhecido e protegido pelo direito da União. Para alcançar esse objetivo, torna-se necessário estabelecer regras aplicáveis à colocação no mercado e à colocação em serviço de determinados sistemas de IA, garantindo assim o correto funcionamento do mercado interno e permitindo que esses sistemas beneficiem do princípio de livre circulação dos produtos e dos serviços. Ao estabelecer essas regras, e com base no trabalho do Grupo de Peritos de Alto Nível em Inteligência Artificial, tal como refletido nas Orientações Éticas para uma IA de Confiança na UE, o presente regulamento apoia o objetivo da União de estar na vanguarda mundial do desenvolvimento de uma inteligência artificial que seja segura, ética e de confiança, conforme mencionado pelo Conselho Europeu[4] e garante a proteção de princípios éticos, conforme solicitado especificamente pelo Parlamento Europeu[5].

---

4 Conselho Europeu, Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) — Conclusões [EUCO 13/20, 2020, p. 6].

5 Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].

(5-A) As regras harmonizadas estabelecidas no presente regulamento relativamente à colocação no mercado, à colocação em serviço e à utilização de sistemas de IA deverão aplicar-se em todos os setores e, em consonância com a abordagem do seu novo quadro legislativo, não deverão prejudicar a legislação da União em vigor, nomeadamente em matéria de proteção de dados, defesa dos consumidores, direitos fundamentais, emprego e segurança dos produtos, com a qual o presente regulamento é complementar. Consequentemente, permanecem inalterados e plenamente aplicáveis todos os direitos e vias de recurso concedidos por essa legislação da União aos consumidores e a outras pessoas que possam ser negativamente afetadas pelos sistemas de IA, nomeadamente no que diz respeito à indemnização por eventuais danos nos termos da Diretiva 85/374/CEE do Conselho, de 25 de julho de 1985, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de responsabilidade decorrente dos produtos defeituosos. Além disso, o presente regulamento visa reforçar a eficácia desses direitos e vias de recurso existentes, estabelecendo requisitos e obrigações específicos, nomeadamente no que diz respeito à transparência, à documentação técnica e à manutenção de registos dos sistemas de IA. Além disso, as obrigações impostas aos vários operadores envolvidos na cadeia de valor da IA ao abrigo do presente regulamento deverão aplicar-se sem prejuízo da legislação nacional, em conformidade com o direito da União, com o efeito de limitar a utilização de determinados sistemas de IA sempre que essa legislação não seja abrangida pelo âmbito de aplicação do presente regulamento ou prossiga outros objetivos legítimos de interesse público para além dos prosseguidos pelo presente regulamento. Por exemplo, o direito do trabalho nacional e a legislação em matéria de proteção de menores (ou seja, pessoas com menos de 18 anos), tendo em conta o Comentário Geral n.º 25 (2021) das Nações Unidas sobre os direitos das crianças, na medida em que não sejam específicos dos sistemas de IA e prossigam outros objetivos legendados de interesse público, não deverão ser afetados pelo presente regulamento.

(6) A definição de "sistema de IA" deverá ser inequívoca, para assegurar a segurança jurídica, concedendo em simultâneo a flexibilidade suficiente para se adaptar a futuras evoluções tecnológicas. A definição deverá basear-se nas principais características funcionais da inteligência artificial, tais como as suas capacidades de aprendizagem, raciocínio ou modelização, distinguindo-a de sistemas de software e abordagens de programação mais simples. Em particular, para efeitos do presente regulamento, os sistemas de IA deverão ter a capacidade de, com base em dados e entradas introduzidos de forma automática e/ou por um ser humano, inferir a forma de alcançar um conjunto de objetivos finais que lhes sejam atribuídos pelos seres humanos, utilizando a aprendizagem automática e/ou abordagens baseadas na lógica e no conhecimento, e produzir resultados tais como conteúdos para sistemas de IA generativa (por exemplo, texto, vídeo ou imagens), previsões, recomendações ou decisões que influenciam o ambiente com o qual o sistema interage, seja numa dimensão física ou digital. Um sistema que utilize regras definidas exclusivamente por pessoas singulares para executar automaticamente operações não deverá ser considerado um sistema de IA. Os sistemas de IA podem ser concebidos para operar com diferentes níveis de autonomia e ser utilizados autonomamente ou como componente de um produto, independentemente de o sistema estar fisicamente incorporado no produto (integrado) ou servir a funcionalidade do produto sem estar incorporado nele (não integrado). O conceito de autonomia de um sistema de IA está relacionado com o grau em que esse sistema funciona sem envolvimento humano.

(6-A) As abordagens de aprendizagem automática centram-se no desenvolvimento de sistemas capazes de aprender e inferir dos dados para resolver um problema de aplicação sem serem explicitamente programados com um conjunto de instruções passo a passo, desde a introdução dos dados até aos resultados. A aprendizagem refere-se ao processo computacional de otimização, a partir de dados, dos parâmetros do modelo, que é uma construção matemática que gera um resultado baseado em dados de entrada. O leque de problemas abordados pela aprendizagem automática envolve normalmente tarefas para as quais outras abordagens falham, quer porque não existe uma formalização adequada do problema, quer porque a resolução do problema é incompatível com abordagens sem aprendizagem. As abordagens de aprendizagem automática incluem, por exemplo, a aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma variedade de métodos que incluem a aprendizagem profunda com redes neuronais, técnicas estatísticas de aprendizagem e inferência (incluindo, por exemplo, a regressão logística, e a estimação de Bayes) e métodos de pesquisa e otimização.

(6-B) As abordagens baseadas na lógica e no conhecimento centram-se no desenvolvimento de sistemas com capacidades de raciocínio lógico sobre os conhecimentos para resolver um problema de aplicação. Esses sistemas envolvem normalmente uma base de conhecimentos e um motor de inferência que gera resultados raciocinando sobre a base de conhecimentos. A base de conhecimentos, que é geralmente codificada por peritos humanos, representa entidades e relações lógicas relevantes para o problema da aplicação através de formalizações baseadas em regras, ontologias ou grafos de conhecimento. O motor de inferência atua na base de conhecimentos e extrai novas informações através de operações como a triagem, a pesquisa, a correspondência ou o encadeamento. As abordagens baseadas na lógica e no conhecimento incluem, por exemplo, a representação do conhecimento, a programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, o raciocínio (simbólico), os sistemas periciais e os métodos de pesquisa e otimização;

(6-C) A fim de assegurar condições uniformes para a execução do presente regulamento no que diz respeito a abordagens de aprendizagem automática e abordagens baseadas na lógica e no conhecimento e de ter em conta a evolução tecnológica e do mercado, deverão ser atribuídas competências de execução à Comissão.

(6-D) O conceito de "utilizador" a que se refere o presente regulamento deverá ser interpretado como qualquer pessoa singular ou coletiva, incluindo uma autoridade pública, agência ou outro organismo, que utilize um sistema de IA sob cuja autoridade o sistema seja utilizado. Dependendo do tipo de sistema de IA, a utilização do sistema pode afetar outras pessoas além do utilizador.

(7) A definição de "dados biométricos" utilizada no presente regulamento deverá ser interpretada de forma coerente com a definição de "dados biométricos" constante do artigo 4.º, ponto 14, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[6], do artigo 3.º, ponto 18, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho[7] e do artigo 3.º, ponto 13, da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho[8].

---

6 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

7 Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

8 Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (Diretiva sobre a Proteção de Dados na Aplicação da Lei) (JO L 119 de 4.5.2016, p. 89).

(8) O conceito de "sistema de identificação biométrica à distância" utilizado no presente regulamento deverá ser definido, de modo funcional, como um sistema de IA que se destina à identificação de pessoas singulares, normalmente à distância, sem o seu envolvimento ativo, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos num repositório de dados de referência, independentemente da tecnologia, dos processos ou dos tipos de dados biométricos utilizados. Esses sistemas de identificação biométrica à distância são geralmente utilizados para detetar (analisar) várias pessoas ou o seu comportamento em simultâneo, a fim de facilitar significativamente a identificação de várias pessoas sem o seu envolvimento ativo. Essa definição exclui os sistemas de verificação/autenticação cujo único objetivo seria confirmar que uma determinada pessoa singular é a pessoa que alega ser, bem como os sistemas utilizados para confirmar a identidade de uma pessoa singular com o único objetivo de lhe conceder acesso a determinado serviço, dispositivo ou instalações. Esta exclusão justifica-se pelo facto de esses sistemas serem suscetíveis de ter um impacto menor nos direitos fundamentais das pessoas singulares em comparação com os sistemas de identificação biométrica à distância que podem ser utilizados para o tratamento de dados biométricos de um grande número de pessoas. No caso dos sistemas "em tempo real", a recolha dos dados biométricos, a comparação e a identificação ocorrem de imediato, quase de imediato ou, em todo o caso, sem um atraso significativo. Não pode haver, a este respeito, margem para contornar as regras do presente regulamento sobre a utilização "em tempo real" dos sistemas de IA em causa por via da introdução de ligeiros retardamentos no sistema. Os sistemas «em tempo real» implicam a utilização "ao vivo" ou "quase ao vivo" de materiais, como vídeos, criados por uma câmara ou outro dispositivo com uma funcionalidade semelhante. Por outro lado, no caso dos sistemas "em diferido", os dados biométricos já foram recolhidos e a comparação e a identificação ocorrem apenas após um atraso significativo. Estes sistemas utilizam materiais, tais como imagens ou vídeos, criados por câmaras de televisão em circuito fechado ou dispositivos privados antes de o sistema ser utilizado relativamente às pessoas singulares em causa.

(9) Para efeitos do presente regulamento, deverá entender-se por "espaço acessível ao público" qualquer espaço físico que seja acessível a um número indeterminado de pessoas singulares, independentemente de o espaço em questão ser detido por uma entidade privada ou pública e independentemente da atividade para a qual o espaço possa ser utilizado – por exemplo, comércio (designadamente lojas, restaurantes, cafés), serviços (designadamente bancos, atividades profissionais, hotelaria), desporto (designadamente piscinas, ginásios, estádios), transportes (designadamente estações de autocarros, metropolitanos e ferroviárias, aeroportos, meios de transporte), entretenimento (designadamente cinemas, teatros, museus, salas de concerto e salas de conferências) ou outros (designadamente estradas, praças, parques, florestas ou parques infantis públicos). Um local também deverá ser classificado como acessível ao público se, independentemente da capacidade potencial ou das restrições de segurança, o acesso estiver sujeito a certas condições predeterminadas, que podem ser preenchidas por um número indeterminado de pessoas, tais como a compra de um bilhete ou título de transporte, a inscrição prévia ou uma determinada idade. Em contrapartida, um local não deverá ser considerado acessível ao público se o acesso for limitado a pessoas singulares específicas e definidas ao abrigo do direito da União ou do direito nacional diretamente relacionado com a segurança pública ou através da manifestação clara de vontade da pessoa que tem a autoridade pertinente no local. A possibilidade factual de acesso por si só (por exemplo, uma porta destrancada ou um portão aberto numa vedação) não implica que o espaço seja acessível ao público na presença de indicações ou circunstâncias que sugiram o contrário (por exemplo, sinais que proíbam ou restrinjam o acesso). As instalações de empresas e fábricas, bem como os escritórios e os locais de trabalho a que se pretende que apenas os trabalhadores e prestadores de serviços pertinentes tenham acesso, são espaços que não são acessíveis ao público. Os espaços acessíveis ao público não deverão incluir prisões ou zonas de controlo fronteiriço. Alguns outros espaços podem ser compostos por zonas não acessíveis ao público e zonas acessíveis ao público, tais como um corredor de um edifício residencial privado necessário para aceder a um gabinete médico ou a um aeroporto. Os espaços em linha também não são abrangidos, uma vez que não são espaços físicos. Para determinar se um espaço é acessível ao público deve recorrer-se a uma análise casuística, tendo em conta as especificidades da situação em apreço.

(10) Para assegurar condições de concorrência equitativas e uma proteção eficaz dos direitos e das liberdades das pessoas singulares em toda a União, as regras estabelecidas no presente regulamento devem aplicar-se aos fornecedores de sistemas de IA de uma forma não discriminatória, independentemente de estarem estabelecidos na União ou num país terceiro, e aos utilizadores de sistemas de IA estabelecidos na União.

(11) Face à natureza digital dos sistemas de IA, determinados sistemas devem ser abrangidos pelo âmbito do presente regulamento, mesmo quando não são colocados no mercado ou em serviço, nem são utilizados na União. Esta situação verifica-se, por exemplo, quando um operador estabelecido na União contrata determinados serviços a um operador estabelecido fora da União relativamente a uma atividade a realizar por um sistema de IA que seria considerado de risco elevado. Nessas circunstâncias, o operador fora da União poderia utilizar o seu sistema de IA para tratar dados recolhidos e transferidos licitamente da União e fornecer ao operador contratante na União o resultado desse sistema de IA decorrente desse tratamento, sem que o sistema de IA em causa fosse colocado no mercado ou em serviço ou utilizado na União. Para evitar que o presente regulamento seja contornado e para assegurar uma proteção eficaz das pessoas singulares localizadas na União, o presente regulamento deve ser igualmente aplicável a fornecedores e utilizadores de sistemas de IA estabelecidos num país terceiro nos casos em que o resultado desses sistemas seja utilizado na União. No entanto, para ter em conta os mecanismos existentes e as necessidades especiais da cooperação futura com os parceiros estrangeiros com quem são trocadas informações e dados, o presente regulamento não deve ser aplicável às autoridades públicas de um país terceiro e às organizações internacionais quando estas atuam no âmbito de acordos internacionais celebrados a nível nacional ou europeu para efeitos de cooperação policial e judiciária com a União ou com os seus Estados-Membros. Tais acordos têm sido celebrados bilateralmente entre Estados-Membros e países terceiros ou entre a União Europeia, a Europol e outras agências da UE e países terceiros e organizações internacionais. As autoridades dos Estados-Membros destinatários e as instituições, órgãos e organismos da União que utilizam esses resultados na União continuam a ser responsáveis por assegurar que a sua utilização é conforme com o direito da União. Quando esses acordos internacionais forem revistos ou forem celebrados novos acordos no futuro, as partes contratantes deverão envidar todos os esforços para alinhar esses acordos com os requisitos do presente regulamento.

(12) O presente regulamento deverá ser também aplicável a instituições, órgãos e organismos da União quando atuam como fornecedor ou utilizador de um sistema de IA.

(12-A) Se e na medida em que os sistemas de IA forem colocados no mercado, colocados em serviço ou utilizados com ou sem modificação desses sistemas para fins militares, de defesa ou de segurança nacional, esses sistemas deverão ser excluídos do âmbito de aplicação do presente regulamento, independentemente do tipo de entidade que realiza essas atividades, por exemplo, seja ela uma entidade pública ou privada. No que diz respeito aos fins militares e de defesa, essa exclusão é justificada tanto pelo artigo 4.º, n.º 2, do TUE como pelas especificidades da política de defesa dos Estados-Membros e da União abrangidas pelo título V, capítulo 2, do Tratado da União Europeia (TUE), que estão sujeitas ao direito internacional público, que é, por conseguinte, o quadro jurídico mais adequado para a regulamentação dos sistemas de IA no contexto da utilização da força letal e de outros sistemas de IA no contexto de atividades militares e de defesa. No que diz respeito aos fins de segurança nacional, a exclusão justifica-se tanto pelo facto de a segurança nacional continuar a ser da exclusiva responsabilidade dos Estados-Membros, em conformidade com o artigo 4.º, n.º 2, do TUE, como pela natureza específica e pelas necessidades operacionais específicas das atividades de segurança nacional e pelas regras nacionais específicas aplicáveis a essas atividades. No entanto, se um sistema de IA desenvolvido, colocado no mercado, colocado em serviço ou utilizado para fins militares, de defesa ou de segurança nacional for utilizado, temporária ou permanentemente, para outros fins (por exemplo, para fins civis ou humanitários, de manutenção da ordem pública ou de segurança pública), será abrangido pelo âmbito de aplicação do presente regulamento. Nesse caso, as entidades que utilizarem o sistema para fins que não sejam fins militares, de defesa ou de segurança nacional deverão assegurar a conformidade do sistema com o presente regulamento, a menos que o sistema já esteja em conformidade com o presente regulamento. Os sistemas de IA colocados no mercado ou colocados em serviço para um fim excluído (ou seja, militar, de defesa ou de segurança nacional) e um ou mais fins não excluídos (por exemplo, fins civis, manutenção da ordem pública, etc.) são abrangidos pelo âmbito de aplicação do presente regulamento e os fornecedores desses sistemas deverão assegurar a conformidade com o presente regulamento. Nesses casos, o facto de um sistema de IA poder ser abrangido pelo âmbito de aplicação do presente regulamento não deverá afetar a possibilidade de as entidades que realizam atividades de segurança nacional, de defesa e militares, independentemente do tipo de entidade que realiza essas atividades, utilizarem sistemas de IA para fins de segurança nacional, militares e de defesa, cuja utilização esteja excluída do âmbito de aplicação do presente regulamento. Um sistema de IA colocado no mercado para fins civis ou de manutenção da ordem pública que seja utilizado com ou sem modificação para fins militares, de defesa ou de segurança nacional não deverá ser abrangido pelo âmbito de aplicação do presente regulamento, independentemente do tipo de entidade que realiza essas atividades.

(12-A) O presente regulamento não prejudica a responsabilidade dos prestadores intermediários de serviços estabelecida na Diretiva 2000/31/CE do Parlamento Europeu e do Conselho [na redação que lhe foi dada pelo Regulamento Serviços Digitais].

(12-B) O presente regulamento não deverá prejudicar as atividades de investigação e desenvolvimento e deverá respeitar a liberdade da ciência. Por conseguinte, é necessário excluir do seu âmbito de aplicação sistemas de IA especificamente desenvolvidos e colocados em serviço exclusivamente para fins de investigação e desenvolvimento científicos e assegurar que o regulamento não afete a atividade de investigação e desenvolvimento científicos em matéria de sistemas de IA. No que diz respeito à atividade de investigação orientada para os produtos por parte dos fornecedores, as disposições do presente regulamento também não deverão ser aplicáveis. Tal não prejudica a obrigação de cumprir o presente regulamento sempre que um sistema de IA abrangido pelo âmbito de aplicação do presente regulamento for colocado no mercado ou colocado em serviço em resultado dessa atividade de investigação e desenvolvimento, nem a aplicação das disposições relativas aos ambientes de testagem da regulamentação e à testagem em condições reais. Além disso, sem prejuízo do que precede no que diz respeito aos sistemas de IA especificamente desenvolvidos e colocados em serviço exclusivamente para fins de investigação e desenvolvimento científicos, qualquer outro sistema de IA que possa ser utilizado para a realização de atividades de investigação e desenvolvimento deverá continuar sujeito às disposições do presente regulamento. Seja em que circunstância for, qualquer atividade de investigação e desenvolvimento deve ser realizada em conformidade com normas éticas e profissionais reconhecidas em matéria de investigação científica.

(12-C) Tendo em conta a natureza e a complexidade da cadeia de valor dos sistemas de IA, é essencial tornar claro o papel dos intervenientes que podem contribuir para o desenvolvimento de sistemas de IA, nomeadamente sistemas de IA de risco elevado. Em especial, é necessário clarificar que os sistemas de IA de finalidade geral são sistemas de IA concebidos pelo fornecedor para desempenhar funções de aplicação geral, como o reconhecimento de imagens/de fala, e em vários contextos. Podem ser utilizados por si próprios como sistemas de IA de risco elevado ou ser componentes de outros sistemas de IA de risco elevado. Por conseguinte, devido à sua natureza específica e a fim de assegurar uma partilha equitativa de responsabilidades ao longo da cadeia de valor da IA, esses sistemas deverão estar sujeitos a requisitos e obrigações proporcionados e mais específicos ao abrigo do presente regulamento, assegurando simultaneamente um elevado nível de proteção dos direitos fundamentais, da saúde e da segurança. Além disso, independentemente de os sistemas de IA de finalidade geral poderem ser utilizados como sistemas de IA de risco elevado enquanto tal por outros fornecedores ou como componentes de sistemas de IA de risco elevado, os fornecedores desses sistemas deverão colaborar, se for caso disso, com os fornecedores dos respetivos sistemas de IA de risco elevado, a fim de permitir a sua conformidade com as obrigações pertinentes previstas no presente regulamento e com as autoridades competentes estabelecidas ao abrigo do presente regulamento. A fim de ter em conta as características específicas dos sistemas de IA de finalidade geral, bem como a rápida evolução do mercado e da tecnologia no terreno, deverão ser atribuídas competências de execução à Comissão para especificar e adaptar a aplicação dos requisitos estabelecidos ao abrigo do presente regulamento aos sistemas de IA de finalidade geral e para especificar as informações a partilhar pelos fornecedores de sistemas de IA de finalidade geral, a fim de permitir que os fornecedores do respetivo sistema de IA de risco elevado cumpram as obrigações que lhes incumbem por força do presente regulamento.

(13) A fim de assegurar um nível elevado e coerente de proteção dos interesses públicos nos domínios da saúde, da segurança e dos direitos fundamentais, devem ser criadas normas comuns aplicáveis a todos os sistemas de IA de risco elevado. Essas normas devem ser coerentes com a Carta dos Direitos Fundamentais da União Europeia (a seguir designada por "Carta") e não discriminatórias, bem como estar em consonância com os compromissos comerciais internacionais da União.

(14) Para que o conjunto de normas vinculativas aplicáveis aos sistemas de IA seja proporcionado e eficaz, deve seguir-se uma abordagem baseada no risco claramente definida. Essa abordagem deve adaptar o tipo e o conteúdo dessas normas à intensidade e ao âmbito dos riscos criados pelos sistemas de IA. Como tal, é necessário proibir determinadas práticas de inteligência artificial, estabelecer requisitos aplicáveis aos sistemas de IA de risco elevado e obrigações para os operadores pertinentes, bem como estabelecer obrigações de transparência para determinados sistemas de IA.

(15) Além das inúmeras utilizações benéficas da inteligência artificial, essa tecnologia pode ser utilizada indevidamente e conceder instrumentos novos e poderosos para práticas manipuladoras, exploratórias e de controlo social. Essas práticas são particularmente prejudiciais e devem ser proibidas, pois desrespeitam valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como direitos fundamentais da União, incluindo o direito à não discriminação, à proteção de dados pessoais e à privacidade, e os direitos das crianças.

(16) As técnicas manipuladoras baseadas na IA podem ser utilizadas para persuadir as pessoas a adotarem comportamentos indesejados, ou para as enganar, incentivando-as a tomar decisões de uma forma que subverta e prejudique a sua autonomia, a sua tomada de decisões e a sua liberdade de escolha. A colocação no mercado, a colocação em serviço ou a utilização de determinados sistemas de IA que distorçam substancialmente o comportamento humano, que sejam passíveis de provocar danos físicos ou psicológicos, são particularmente perigosas e deverão, por isso, ser proibidas. Esses sistemas de IA utilizam componentes subliminares, como os estímulos de áudio, de imagem e de vídeo, que as pessoas não conseguem perceber enquanto tal dado que esses estímulos ultrapassam a perceção humana, ou outras técnicas subliminares que subvertem ou prejudicam a autonomia, a tomada de decisões ou a liberdade de escolha das pessoas de forma a que as pessoas não estejam conscientemente cientes, ou, mesmo que o estejam, não sejam capazes de se controlar ou de lhes resistir; é, por exemplo, o caso das interfaces máquina-cérebro ou da realidade virtual. Além disso, os sistemas de IA podem também explorar vulnerabilidades de um grupo específico de pessoas devido à sua idade, à sua deficiência na aceção da Diretiva (UE) 2019/882, ou a uma situação social ou económica específica suscetível de tornar essas pessoas mais vulneráveis à exploração, como as pessoas que vivem em situação de pobreza extrema ou minorias étnicas ou religiosas. Esses sistemas de IA podem ser colocados no mercado, colocados em serviço ou utilizados com o objetivo ou o efeito de distorcer substancialmente o comportamento de uma pessoa e de uma forma que cause ou seja razoavelmente suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa ou grupos de pessoas, incluindo danos que possam ser acumulados ao longo do tempo. A intenção de distorcer o comportamento pode não ser presumida se a distorção resultar de fatores externos ao sistema de IA que estão fora do controlo do fornecedor ou do utilizador, ou seja, fatores que podem não ser razoavelmente previstos e atenuados pelo fornecedor ou utilizador do sistema de IA. De qualquer modo, não é necessário que o fornecedor ou o utilizador tenham a intenção de causar os danos físicos ou psicológicos; basta que tal dano resulte das práticas manipuladoras ou exploratórias baseadas na IA. As proibições de tais práticas de IA complementam as disposições da Diretiva 2005/29/CE, nomeadamente as que proíbem as práticas comerciais desleais que causam danos económicos ou financeiros aos consumidores, em quaisquer circunstâncias, independentemente de serem aplicadas através de sistemas de IA ou de outra forma. As proibições de práticas manipuladoras e exploratórias previstas no presente regulamento não deverão afetar as práticas lícitas no contexto de tratamentos médicos, como o tratamento psicológico de uma doença mental ou a reabilitação física, sempre que tais práticas forem realizadas em conformidade com as normas e a legislação médicas aplicáveis. Além disso, as práticas comerciais comuns e legítimas que estejam em conformidade com a legislação aplicável não deverão, por si só, ser consideradas práticas manipuladoras prejudiciais de IA.

(17) Os sistemas de IA que possibilitam a classificação social de pessoas singulares pelas autoridades públicas ou por intervenientes privados podem criar resultados discriminatórios e levar à exclusão de determinados grupos. Estes sistemas podem ainda violar o direito à dignidade e à não discriminação e os valores da igualdade e da justiça. Esses sistemas de IA avaliam ou classificam pessoas singulares com base no seu comportamento social em diversos contextos ou em características de personalidade ou pessoais, conhecidas ou previsíveis. A classificação social obtida por meio desses sistemas de IA pode levar ao tratamento prejudicial ou desfavorável de pessoas singulares ou grupos inteiros das mesmas em contextos sociais não relacionados com o contexto nos quais os dados foram originalmente gerados ou recolhidos ou a um tratamento prejudicial que é injustificado ou desproporcionado face à gravidade do seu comportamento social. Como tal, os sistemas de IA que impliquem tais práticas de classificação inaceitáveis deverão ser proibidos. Essa proibição não deverá afetar as práticas de avaliação lícitas de pessoas singulares efetuadas para um ou mais fins específicos, em conformidade com a lei.

(18) A utilização de sistemas de IA para a identificação biométrica à distância "em tempo real" de pessoas singulares em espaços acessíveis ao público para efeitos de manutenção da ordem pública é considerada particularmente intrusiva para os direitos e as liberdades das pessoas em causa, visto que pode afetar a vida privada de uma grande parte da população, dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais. Além disso, dado o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções da utilização desses sistemas que funcionam "em tempo real", estes dão origem a riscos acrescidos para os direitos e as liberdades das pessoas visadas pelas autoridades policiais.

(19) Como tal, deverá ser proibida a utilização desses sistemas para efeitos de manutenção da ordem pública, salvo em situações enunciadas exaustivamente e definidas de modo restrito, em que a utilização é estritamente necessária por motivos de interesse público importante e cuja importância prevalece sobre os riscos. Essas situações implicam a procura de potenciais vítimas de crimes, incluindo crianças desaparecidas, certas ameaças à vida ou à segurança física de pessoas singulares ou ameaças de ataque terrorista, e a deteção, localização, identificação ou instauração de ações penais relativamente a infratores ou suspeitos de infrações penais a que se refere a Decisão-Quadro 2002/584/JAI[9] do Conselho, desde que puníveis no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro. Esse limiar para a pena ou medida de segurança privativa de liberdade prevista no direito nacional contribui para assegurar que a infração seja suficientemente grave para justificar potencialmente a utilização de sistemas de identificação biométrica à distância "em tempo real". Além disso, das 32 infrações penais enumeradas na Decisão-Quadro 2002/584/JAI do Conselho, algumas são provavelmente mais pertinentes do que outras, já que o recurso à identificação biométrica à distância "em tempo real" será previsivelmente necessário e proporcionado em graus extremamente variáveis no respeitante à deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito das diferentes infrações penais enumeradas e tendo em conta as prováveis diferenças em termos de gravidade, probabilidade e magnitude dos prejuízos ou das possíveis consequências negativas. Além disso, o presente regulamento deverá preservar a capacidade das autoridades competentes em matéria de manutenção da ordem pública, controlo das fronteiras, imigração ou asilo para realizarem controlos de identidade na presença da pessoa em causa, em conformidade com as condições estabelecidas no direito da União e no direito nacional para esses controlos. Em especial, as autoridades competentes em matéria de manutenção da ordem pública, controlo das fronteiras, imigração ou asilo deverão poder utilizar sistemas de informação, em conformidade com o direito da União ou o direito nacional, para identificar uma pessoa que, durante um controlo de identidade, se recuse a ser identificada ou não seja capaz de declarar ou provar a sua identidade, sem serem obrigadas a obter uma autorização prévia por força do presente regulamento. Pode tratar-se, por exemplo, de uma pessoa envolvida num crime, ou que não queira ou não possa, devido a um acidente ou a uma situação médica, divulgar a sua identidade às autoridades policiais.

---

[9] Decisão-quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO L 190 de 18.7.2002, p. 1).

(20) A fim de assegurar que esses sistemas sejam utilizados de uma forma responsável e proporcionada, também importa estabelecer que, em cada uma dessas situações enunciadas exaustivamente e definidas de modo restrito, é necessário ter em conta determinados elementos, em especial no que se refere à natureza da situação que dá origem ao pedido e às consequências da utilização para os direitos e as liberdades de todas as pessoas em causa e ainda às salvaguardas e condições previstas para a utilização. Além disso, a utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública deve estar sujeita a limites espaciais e temporais adequados, tendo em conta, especialmente, os dados ou indícios relativos às ameaças, às vítimas ou ao infrator. A base de dados de pessoas utilizada como referência deverá ser adequada a cada utilização em cada uma das situações acima indicadas.

(21) Cada utilização de um sistema de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública deve estar sujeita a uma autorização expressa e específica de uma autoridade judiciária ou de uma autoridade administrativa independente de um Estado-Membro. Em princípio, essa autorização deverá ser obtida antes da utilização do sistema com vista a identificar uma ou várias pessoas. Deverão ser permitidas exceções a essa regra em situações de urgência devidamente justificadas, ou seja, quando a necessidade de utilizar os sistemas em causa torna efetiva e objetivamente impossível obter uma autorização antes de iniciar essa utilização. Nessas situações de urgência, a utilização deve limitar-se ao mínimo absolutamente necessário e estar sujeita a salvaguardas e condições adequadas, conforme determinado pelo direito nacional e especificado no contexto de cada caso de utilização urgente pela própria autoridade policial. Ademais, nessas situações, a autoridade policial deve procurar obter quanto antes uma autorização, apresentando as razões para não ter efetuado o pedido mais cedo.

(22) Além disso, no âmbito do quadro exaustivo estabelecido pelo presente regulamento, importa salientar que essa utilização no território de um Estado-Membro apenas deve ser possível uma vez que o Estado-Membro em causa tenha decidido possibilitar expressamente a autorização dessa utilização de acordo com o presente regulamento nas regras de execução previstas no direito nacional. Consequentemente, ao abrigo do presente regulamento, os Estados-Membros continuam a ser livres de não possibilitar essa utilização ou de apenas possibilitar essa utilização relativamente a alguns dos objetivos passíveis de justificar uma utilização autorizada identificados no presente regulamento.

(23) A utilização de sistemas de IA para a identificação biométrica à distância "em tempo real" de pessoas singulares em espaços acessíveis ao público para efeitos de manutenção da ordem pública implica necessariamente o tratamento de dados biométricos. As regras do presente regulamento que proíbem essa utilização, salvo em certas exceções, e que têm por base o artigo 16.º do TFUE, deverão aplicar-se como *lex specialis* relativamente às regras em matéria de tratamento de dados biométricos previstas no artigo 10.º da Diretiva (UE) 2016/680, regulando assim essa utilização e o tratamento de dados biométricos conexo de uma forma exaustiva. Como tal, essa utilização e esse tratamento apenas devem ser possíveis se forem compatíveis com o quadro estabelecido pelo presente regulamento, sem que exista margem, fora desse quadro, para as autoridades competentes utilizarem esses sistemas e efetuarem o tratamento desses dados pelos motivos enunciados no artigo 10.º da Diretiva (UE) 2016/680, caso atuem para efeitos de manutenção da ordem pública. Neste contexto, o presente regulamento não pretende constituir o fundamento jurídico do tratamento de dados pessoais, nos termos do artigo 8.º da Diretiva (UE) 2016/680. Contudo, a utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para outros fins que não os policiais, incluindo por parte das autoridades competentes, não deve ser abrangida pelo quadro específico relativo a essa utilização para efeitos de manutenção da ordem pública estabelecido pelo presente regulamento. Assim, uma utilização para outros fins que não a manutenção da ordem pública não deve estar sujeita ao requisito de autorização previsto no presente regulamento nem às eventuais regras de execução previstas no direito nacional.

(24) Qualquer tratamento de dados biométricos e de outros dados pessoais envolvidos na utilização de sistemas de IA para fins de identificação biométrica, desde que não estejam associados à utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública, conforme regida pelo presente regulamento deverá continuar a cumprir todos os requisitos decorrentes do artigo10.º da Diretiva (UE) 2016/680. Para outros fins que não a manutenção da ordem pública, o artigo 9.º, n.º 1, do Regulamento (UE) 2016/679 e o artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725 proíbem o tratamento de dados biométricos identificar uma pessoa de forma inequívoca, a menos que se verifique um dos casos previstos no segundo parágrafo desses dois artigos.

(25) Nos termos do artigo 6.º-A do Protocolo (n.º 21) relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, a Irlanda não fica vinculada pelas regras estabelecidas no artigo 5.º, n.º 1, alínea d), e n.ºs 2, 3 e 4, do presente regulamento e adotadas com base no artigo 16.º do TFUE que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades que se enquadram no âmbito da parte III, título V, capítulos 4 ou 5, do TFUE, caso não esteja vinculada por regras que rejam formas de cooperação judiciária em matéria penal ou de cooperação policial no âmbito das quais devam ser observadas as disposições definidas com base no artigo 16.º do TFUE.

(26) Nos termos dos artigos 2.º e 2.º-A do Protocolo (n.º 22) relativo à posição da Dinamarca, anexo ao TUE e ao TFUE, a Dinamarca não fica vinculada pelas regras estabelecidas no artigo 5.º, n.º 1, alínea d), e n.ºs 2, 3 e 4, do presente regulamento e adotadas com base no artigo 16.º do TFUE que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades que se enquadram no âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, nem fica sujeita à aplicação das mesmas.

(27) Os sistemas de IA de risco elevado só podem ser colocados no mercado da União ou colocados em serviço se cumprirem determinados requisitos obrigatórios. Esses requisitos devem assegurar que os sistemas de IA de risco elevado disponíveis na União ou cujos resultados sejam utilizados na União não representam riscos inaceitáveis para interesses públicos importantes da União, conforme reconhecidos e protegidos pelo direito da União. A classificação de "risco elevado" aplicada a sistemas de IA deve limitar-se aos sistemas que têm um impacto prejudicial substancial na saúde, na segurança e nos direitos fundamentais das pessoas no território da União e essa limitação deve minimizar quaisquer potenciais restrições ao comércio internacional, se for caso disso.

(28) Os sistemas de IA podem produzir resultados adversos para a saúde e a segurança das pessoas, em particular quando esses sistemas funcionam como componentes de produtos. Em conformidade com os objetivos da legislação de harmonização da União, designadamente facilitar a livre circulação de produtos no mercado interno e assegurar que apenas os produtos seguros e conformes entram no mercado, é importante prevenir e atenuar devidamente os riscos de segurança que possam ser criados por um produto devido aos seus componentes digitais, incluindo sistemas de IA. A título de exemplo, os robôs, que se têm tornado cada vez mais autónomos, devem operar com segurança e realizar as suas funções em ambientes complexos, seja num contexto industrial ou de assistência e cuidados pessoais. De igual forma, no setor da saúde, em que os riscos para a vida e a saúde são particularmente elevados, os cada vez mais sofisticados sistemas de diagnóstico e sistemas que apoiam decisões humanas devem produzir resultados exatos e de confiança. A dimensão dos impactos adversos causados pelo sistema de IA nos direitos fundamentais protegidos pela Carta é particularmente importante quando se classifica um sistema de IA como sendo de risco elevado. Esses direitos incluem o direito à dignidade do ser humano, o respeito da vida privada e familiar, a proteção de dados pessoais, a liberdade de expressão e de informação, a liberdade de reunião e de associação, a não discriminação, a defesa dos consumidores, os direitos dos trabalhadores, os direitos das pessoas com deficiência, o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa e o direito a uma boa administração. Além desses direitos, é importante salientar que as crianças têm direitos específicos, consagrados no artigo 24.º da Carta da UE e na Convenção das Nações Unidas sobre os Direitos da Criança (descritos em mais pormenor no Comentário geral n.º 25 da Convenção das Nações Unidas sobre os Direitos da Criança no respeitante ao ambiente digital), que exigem que as vulnerabilidades das crianças sejam tidas em conta e que estas recebam a proteção e os cuidados necessários ao seu bem-estar. O direito fundamental a um nível elevado de proteção do ambiente consagrado na Carta e aplicado nas políticas da União também deve ser tido em conta ao avaliar a gravidade dos danos que um sistema de IA pode causar, incluindo em relação à saúde e à segurança das pessoas.

(29) Relativamente aos sistemas de IA de risco elevado que são componentes de segurança de produtos ou sistemas ou que são, eles próprios, produtos ou sistemas abrangidos pelo âmbito do Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho[10], do Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho[11], do Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho[12], da Diretiva 2014/90/UE do Parlamento Europeu e do Conselho[13], da Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho[14], do Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho[15], do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho[16] e do Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho[17], é adequado alterar esses atos para assegurar que a Comissão tenha em conta, aquando da adoção de futuros atos delegados ou de execução baseados nesses atos, os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado estabelecidos no presente regulamento, atendendo às especificidades técnicas e regulamentares de cada setor e sem interferir com os mecanismos de governação, de avaliação da conformidade e de execução existentes nem com as autoridades estabelecidas nestes regulamentos.

---

10 Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).

11 Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho, de 5 de fevereiro de 2013, relativo à homologação e fiscalização do mercado de tratores agrícolas e florestais (JO L 60 de 2.3.2013, p. 1).

12 Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação e fiscalização do mercado dos veículos de duas ou três rodas e dos quadriciclos (JO L 60 de 2.3.2013, p. 52).

13 Diretiva 2014/90/UE do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativa aos equipamentos marítimos e que revoga a Diretiva 96/98/CE do Conselho (JO L 257 de 28.8.2014, p. 146).

14 Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, relativa à interoperabilidade do sistema ferroviário na União Europeia (JO L 138 de 26.5.2016, p. 44).

15 Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativo à homologação e à fiscalização do mercado dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a esses veículos, que altera os Regulamentos (CE) n.º 715/2007 e (CE) n.º 595/2009 e revoga a Diretiva 2007/46/CE (JO L 151 de 14.6.2018, p. 1).

16 Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, de 4 de julho de 2018, relativo a regras comuns no domínio da aviação civil que cria a Agência da União Europeia para a Segurança da Aviação, altera os Regulamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010 e (UE) n.º 376/2014 e as Diretivas 2014/30/UE e 2014/53/UE do Parlamento Europeu e do Conselho, e revoga os Regulamentos (CE) n.º 552/2004 e (CE) n.º 216/2008 do Parlamento Europeu e do Conselho e o Regulamento (CEE) n.º 3922/91 do Conselho (JO L 212 de 22.8.2018, p. 1).

17 Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativo aos requisitos de homologação de veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos, no que se refere à sua segurança geral e à proteção dos ocupantes dos veículos e dos utentes da estrada vulneráveis, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 78/2009, (CE) n.º 79/2009 e (CE) n.º 661/2009 do Parlamento Europeu e do Conselho e os Regulamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012, e (UE) 2015/166 da Comissão (JO L 325 de 16.12.2019, p. 1).

(30) Relativamente aos sistemas de IA que são componentes de segurança de produtos ou que são, eles próprios, produtos abrangidos pelo âmbito de determinada legislação de harmonização da União, é apropriado classificá-los como de risco elevado ao abrigo do presente regulamento nos casos em que forem objeto de um procedimento de avaliação da conformidade realizado por um organismo terceiro de avaliação da conformidade nos termos dessa legislação de harmonização da União aplicável. Em particular, tais produtos são máquinas, brinquedos, ascensores, aparelhos e sistemas de proteção destinados a ser utilizados em atmosferas potencialmente explosivas, equipamentos de rádio, equipamentos sob pressão, equipamentos de embarcações de recreio, instalações por cabo, aparelhos a gás, dispositivos médicos e dispositivos médicos para diagnóstico in vitro.

(31) Classificar um sistema de IA como de risco elevado nos termos do presente regulamento não implica necessariamente que o produto cujo componente de segurança é o sistema de IA ou que o próprio sistema de IA enquanto produto seja considerado «de risco elevado», segundo os critérios estabelecidos na legislação de harmonização da União aplicável ao produto. Tal verifica-se no respeitante ao Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho[18] e ao Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho[19], que preveem a avaliação por terceiros da conformidade de produtos de risco médio e elevado.

---

18 Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho (JO L 117 de 5.5.2017, p. 1).

19 Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos para diagnóstico *in vitro* e que revoga a Diretiva 98/79/CE e a Decisão 2010/227/UE da Comissão (JO L 117 de 5.5.2017, p. 176).

(32) Relativamente aos sistemas de IA de risco elevado que não são componentes de segurança de produtos nem são, eles próprios, produtos, é apropriado classificá-los como de risco elevado se, em função da finalidade prevista, representarem um risco elevado de danos para a saúde e a segurança ou de prejuízo para os direitos fundamentais das pessoas, tendo em conta a gravidade dos possíveis danos e a probabilidade dessa ocorrência, e se forem utilizados num conjunto de domínios especificamente predefinidos no regulamento. A identificação desses sistemas baseia-se na mesma metodologia e nos mesmos critérios previstos para futuras alterações da lista de sistemas de IA de risco elevado. É igualmente importante esclarecer que, nos cenários de risco elevado referidos no anexo III, podem existir sistemas que não conduzam a um risco significativo para os interesses jurídicos protegidos nesses cenários, tendo em conta os resultados produzidos pelo sistema de IA. Por conseguinte, o sistema de IA que gera esses resultados apenas deverá ser considerado de risco elevado quando esses resultados têm um elevado grau de importância (ou seja, não são puramente acessórios) no que diz respeito à ação ou decisão em causa, de modo a gerar um risco significativo para os interesses jurídicos protegidos. Por exemplo, quando as informações fornecidas por um sistema de IA ao ser humano consistem na definição de perfis de pessoas singulares na aceção do artigo 4.º, n.º 4, do Regulamento (UE) 2016/679, do artigo 3.º, n.º 4, da Diretiva (UE) 2016/680 e do artigo 3.º, n.º 5, do Regulamento (UE) 2018/1725, essas informações não deverão normalmente ser consideradas de natureza acessória no contexto dos sistemas de IA de risco elevado a que se refere o anexo III. No entanto, se o resultado do sistema de IA tiver apenas uma relevância negligenciável ou ínfima para a ação ou decisão humana, pode ser considerado meramente acessório, incluindo, por exemplo, sistemas de IA utilizados para tradução para fins informativos ou para a gestão de documentos.

(33) As imprecisões técnicas dos sistemas de IA concebidos para a identificação biométrica à distância de pessoas singulares podem conduzir a resultados enviesados e ter efeitos discriminatórios. Esta questão é particularmente importante no que diz respeito à idade, à raça, à etnia, ao sexo ou a deficiências das pessoas. Como tal, os sistemas de identificação biométrica à distância "em tempo real" e "em diferido" devem ser classificados como de risco elevado. Face aos riscos que estes dois tipos de sistemas de identificação biométrica à distância representam, ambos devem estar sujeitos a requisitos específicos relativos às capacidades de registo e à supervisão humana.

(34) No tocante à gestão e ao funcionamento de infraestruturas críticas, é apropriado classificar como sendo de risco elevado os sistemas de IA concebidos para serem utilizados como componentes de segurança na gestão e no funcionamento das infraestruturas digitais críticas conforme definidas no anexo I, ponto 8, da Diretiva relativa à resiliência das entidades críticas, do tráfego rodoviário e das redes de abastecimento de água, gás, aquecimento e eletricidade, uma vez que a falha ou anomalia destes sistemas pode pôr em risco a vida e a saúde das pessoas em larga escala e provocar perturbações substanciais das atividades sociais e económicas normais. Os componentes de segurança das infraestruturas críticas, incluindo as infraestruturas digitais críticas, são sistemas utilizados para proteger diretamente a integridade física das infraestruturas críticas ou a saúde e a segurança das pessoas e dos bens, mas que não são necessários para o funcionamento do sistema. A falha ou a anomalia desses componentes podem conduzir diretamente a riscos para a integridade física das infraestruturas críticas e, por conseguinte, a riscos para a saúde e a segurança das pessoas e dos bens. Os componentes destinados a serem utilizados exclusivamente para fins de cibersegurança não deverão ser considerados componentes de segurança. Os exemplos de componentes de segurança dessas infraestruturas críticas podem incluir sistemas de monitorização da pressão da água ou sistemas de controlo de alarmes de incêndio em centros de computação em nuvem.

(35) Os sistemas de IA utilizados no domínio da educação ou formação profissional, designadamente para determinar o acesso, a admissão ou a afetação de pessoas a instituições de ensino e de formação profissional ou a programas de todos os níveis, ou para avaliar resultados de aprendizagem de pessoas, deverão ser considerados de risco elevado, uma vez que determinam o percurso académico e profissional das pessoas e, como tal, afetam a capacidade destas para garantir a subsistência. Se indevidamente concebidos e utilizados, estes sistemas podem violar o direito à educação e à formação, bem como o direito a não ser alvo de discriminação e de perpetuação de padrões históricos de discriminação.

(36) Os sistemas de IA utilizados nos domínios do emprego, da gestão de trabalhadores e do acesso ao emprego por conta própria, nomeadamente para efeitos de recrutamento e seleção, de tomada de decisões sobre promoções e despedimentos, de repartição de tarefas com base em comportamentos individuais ou traços ou características de personalidade, e de controlo ou avaliação de pessoas no âmbito de relações contratuais de trabalho também devem ser classificados como de risco elevado, uma vez que podem ter um impacto significativo nas perspetivas de carreira e na subsistência dessas pessoas. O conceito de "relações contratuais relacionadas com o trabalho" deve abranger os funcionários e as pessoas que prestam serviços por intermédio de plataformas, conforme mencionado no programa de trabalho da Comissão para 2021. Em princípio, essas pessoas não devem ser consideradas "utilizadores" na aceção do presente regulamento. Ao longo do processo de recrutamento e na avaliação, promoção ou retenção de pessoas em relações contratuais relacionadas com o trabalho, esses sistemas podem perpetuar padrões históricos de discriminação, por exemplo, contra as mulheres, certos grupos etários, pessoas com deficiência ou pessoas de uma determinada origem racial ou étnica ou orientação sexual. Os sistemas de IA utilizados para controlar o desempenho e o comportamento destas pessoas podem ter ainda um impacto nos seus direitos à proteção de dados pessoais e à privacidade.

(37) Outro domínio no qual a utilização de sistemas de IA merece especial atenção é o acesso a determinados serviços e prestações essenciais, de cariz privado e público, e o usufruto dos mesmos, os quais são necessários para que as pessoas participem plenamente na sociedade ou melhorem o seu nível de vida. Em particular, os sistemas de IA utilizados para avaliar a classificação de crédito ou a capacidade de endividamento de pessoas singulares devem ser classificados como sistemas de IA de risco elevado, uma vez que determinam o acesso dessas pessoas a recursos financeiros ou a serviços essenciais, como o alojamento, a eletricidade e os serviços de telecomunicações. Os sistemas de IA utilizados para essa finalidade podem conduzir à discriminação de pessoas ou grupos e perpetuar padrões históricos de discriminação, por exemplo, em razão da origem étnica ou racial, deficiência, idade ou orientação sexual, ou criar novas formas de impactos discriminatórios. Tendo em conta a dimensão bastante limitada do impacto e as alternativas disponíveis no mercado, é apropriado isentar os sistemas de IA utilizados para efeitos de avaliação da capacidade de endividamento e de classificação de crédito que sejam colocados em serviço por micro ou pequenas empresas, conforme definidas no anexo da Recomendação da Comissão 2003/361/CE, para utilização própria. Normalmente, as pessoas singulares que se candidatam ou que recebem prestações e serviços de assistência pública essenciais de autoridades públicas dependem dos mesmos e estão numa posição vulnerável face às autoridades competentes. Caso sejam utilizados para determinar a recusa, redução, revogação ou recuperação dessas prestações e serviços pelas autoridades, nomeadamente para determinar se os beneficiários têm legítimo direito a essas prestações e serviços, os sistemas de IA podem ter um impacto significativo na subsistência das pessoas e podem infringir os seus direitos fundamentais, como o direito à proteção social, à não discriminação, à dignidade do ser humano ou à ação. Como tal, esses sistemas devem ser classificados como de risco elevado. No entanto, o presente regulamento não pode constituir um obstáculo ao desenvolvimento e à utilização de abordagens inovadoras na administração pública, que tirariam partido de uma maior utilização de sistemas de IA conformes e seguros, desde que esses sistemas não representem um risco elevado para as pessoas coletivas e singulares. Por último, os sistemas de IA utilizados para enviar ou estabelecer prioridades no envio de serviços de resposta a emergências devem ser classificados como de risco elevado, uma vez que tomam decisões em situações bastante críticas que afetam a vida, a saúde e os bens das pessoas. Os sistemas de IA são também cada vez mais utilizados nas avaliações de risco em relação a pessoas singulares e na fixação de preços de seguros de vida e de saúde que, se não forem devidamente concebidos, desenvolvidos e utilizados, podem ter consequências graves para a vida e a saúde das pessoas, incluindo a exclusão financeira e a discriminação. A fim de assegurar uma abordagem coerente no setor dos serviços financeiros, deverá aplicar-se a exceção acima referida às micro ou pequenas empresas em caso de uso próprio, na medida em que elas próprias forneçam e coloquem em serviço um sistema de IA para efeitos de venda dos seus próprios produtos de seguros.

(38) As ações das autoridades policiais que implicam certas utilizações dos sistemas de IA são caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem como ter outros impactos adversos nos direitos fundamentais garantidos pela Carta. Em particular, se não for treinado com dados de alta qualidade, não cumprir os requisitos adequados em termos de exatidão ou solidez ou não tiver sido devidamente concebido e testado antes de ser colocado no mercado ou em serviço, o sistema de IA pode destacar pessoas de uma forma discriminatória ou incorreta e injusta. Além disso, o exercício de importantes direitos fundamentais processuais, como o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa, pode ser prejudicado, em particular, se esses sistemas de IA não forem suficientemente transparentes, explicáveis e documentados. Como tal, é apropriado classificar como de risco elevado um conjunto de sistemas de IA concebidos para serem utilizados no contexto da manutenção da ordem pública, no qual a exatidão, a fiabilidade e a transparência são particularmente importantes para evitar impactos adversos, reter a confiança do público e assegurar a responsabilidade e vias de recurso eficazes. Tendo em conta a natureza das atividades em causa e os riscos associados às mesmas, esses sistemas de IA de risco elevado deverão incluir, em particular, sistemas de IA concebidos para serem utilizados pelas autoridades policiais em avaliações individuais de riscos, em polígrafos e em instrumentos semelhantes ou para detetar o estado emocional de uma pessoa singular, para avaliar a fiabilidade dos elementos de prova em processos penais, para prever a ocorrência ou a recorrência de uma infração penal real ou potencial com base na definição de perfis de pessoas singulares ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos, para a definição de perfis no decurso da deteção, investigação ou repressão de infrações penais. Os sistemas de IA especificamente concebidos para serem utilizados em processos administrativos por autoridades fiscais e aduaneiras, bem como por unidades de informação financeira que realizem tarefas administrativas de análise de informações nos termos da legislação da União em matéria de combate ao branqueamento de capitais, não devem ser considerados sistemas de IA de risco elevado utilizados por autoridades policiais para efeitos de prevenção, deteção, investigação e repressão de infrações penais.

(39) Os sistemas de IA utilizados na gestão da migração, do asilo e do controlo das fronteiras afetam pessoas que, muitas vezes, se encontram numa posição particularmente vulnerável e que dependem do resultado das ações das autoridades públicas competentes. Como tal, a exatidão, a natureza não discriminatória e a transparência dos sistemas de IA utilizados nesses contextos são particularmente importantes para garantir o respeito dos direitos fundamentais das pessoas em causa, nomeadamente os seus direitos à livre circulação, à não discriminação, à proteção da vida privada e dos dados pessoais, à proteção internacional e a uma boa administração. Deste modo, é apropriado classificar como de risco elevado os sistemas de IA concebidos para serem utilizados por autoridades públicas competentes incumbidas de funções no domínio da gestão da migração, do asilo e do controlo das fronteiras, como polígrafos e instrumentos semelhantes, ou para detetar o estado emocional de uma pessoa singular; para avaliar determinados riscos colocados pelas pessoas singulares que entram no território de um Estado-Membro ou pedem um visto ou asilo; para auxiliar as autoridades públicas competentes na análise dos pedidos de asilo, de visto e de autorização de residência e das queixas relacionadas, com o objetivo de estabelecer a elegibilidade das pessoas singulares que requerem determinado estatuto. Os sistemas de IA no domínio da gestão da migração, do asilo e do controlo das fronteiras abrangidos pelo presente regulamento devem cumprir os requisitos processuais estabelecidos na Diretiva 2013/32/UE do Parlamento Europeu e do Conselho[20], no Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho[21] e noutra legislação aplicável.

---

20 Diretiva 2013/32/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa a procedimentos comuns de concessão e retirada do estatuto de proteção internacional (JO L 180 de 29.6.2013, p. 60).

21 Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que estabelece o Código Comunitário de Vistos (Código de Vistos) (JO L 243 de 15.9.2009, p. 1).

(40) Determinados sistemas de IA concebidos para a administração da justiça e os processos democráticos devem ser classificados como de risco elevado, tendo em conta o seu impacto potencialmente significativo na democracia, no Estado de direito e nas liberdades individuais, bem como no direito à ação e a um tribunal imparcial. Em particular, para fazer face aos riscos de potenciais enviesamentos, erros e opacidade, é apropriado classificar como de risco elevado os sistemas de IA concebidos para auxiliar as autoridades judiciárias na interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos. Contudo, essa classificação não deverá ser alargada aos sistemas de IA concebidos para atividades administrativas puramente auxiliares que não afetam a administração efetiva da justiça em casos individuais, como a anonimização ou a pseudonimização de decisões judiciais, documentos ou dados, comunicações entre pessoal ou tarefas administrativas.

(41) A classificação de um sistema de IA como de risco elevado por força do presente regulamento não deverá ser interpretada como uma indicação de que a utilização do sistema é lícita ao abrigo de outros atos do direito da União ou ao abrigo do direito nacional compatível com o direito da União, por exemplo, em matéria de proteção de dados pessoais ou de utilização de polígrafos e de instrumentos semelhantes ou de outros sistemas para detetar o estado emocional de pessoas singulares. Essa utilização deve continuar sujeita ao cumprimento dos requisitos aplicáveis resultantes da Carta e dos atos do direito derivado da União e do direito nacional em vigor. O presente regulamento não pode ser entendido como um fundamento jurídico para o tratamento de dados pessoais, incluindo de categorias especiais de dados pessoais, se for caso disso, salvo disposição específica em contrário no presente regulamento.

(42) Para atenuar os riscos dos sistemas de IA de risco elevado colocados no mercado ou colocados em serviço no mercado da União, deverão aplicar-se determinados requisitos obrigatórios, tendo em conta a finalidade de utilização prevista do sistema e de acordo com o sistema de gestão de riscos a estabelecer pelo fornecedor. Em particular, o sistema de gestão de riscos deverá consistir num processo iterativo contínuo, planeado e executado ao longo de todo o ciclo de vida de um sistema de IA de risco elevado. Esse processo deverá assegurar que o fornecedor identifica e analisa os riscos para a saúde, a segurança e os direitos fundamentais das pessoas que possam ser afetadas pelo sistema à luz da sua finalidade prevista, incluindo os eventuais riscos decorrentes da interação entre o sistema de IA e o ambiente em que opera, e, por conseguinte, adota medidas de gestão dos riscos adequadas, à luz do estado da técnica.

(43) Os sistemas de IA de risco elevado devem estar sujeitos ao cumprimento de requisitos relativos à qualidade dos conjuntos de dados utilizados, à documentação técnica e à manutenção de registos, à transparência e à prestação de informações aos utilizadores, à supervisão humana, à solidez, à exatidão e à cibersegurança. Esses requisitos são necessários para atenuar eficazmente os riscos para a saúde, a segurança e os direitos fundamentais, em função da finalidade prevista do sistema e quando não existam outras medidas menos restritivas do comércio, evitando, assim, restrições injustificadas do comércio.

(44) A disponibilidade de dados de elevada qualidade é um fator essencial para o desempenho de vários sistemas de IA, sobretudo quando são utilizadas técnicas que envolvem o treino de modelos, com vista a assegurar que o sistema de IA de risco elevado funcione como pretendido e de modo seguro e não se torne a fonte de uma discriminação proibida pelo direito da União. Para garantir conjuntos de dados de treino, validação e testagem de elevada qualidade é necessário aplicar práticas adequadas de governação e gestão de dados. Os conjuntos de dados de treino, validação e testagem deverão ser suficientemente relevantes e representativos, e ter as propriedades estatísticas adequadas, nomeadamente no que respeita às pessoas ou aos grupos de pessoas nos quais o sistema de IA de risco elevado será utilizado. Estes conjuntos de dados deverão também ser, tanto quanto possível, isentos de erros e completos, na perspetiva da finalidade prevista do sistema de IA, tendo em conta, de forma proporcionada, a viabilidade técnica e o estado da técnica, a disponibilidade de dados e a aplicação de medidas de gestão dos riscos adequadas, para que as eventuais insuficiências dos conjuntos de dados sejam devidamente colmatadas. O requisito de os conjuntos de dados estarem completos e isentos de erros não deverá afetar a utilização de técnicas de preservação da privacidade no contexto do desenvolvimento e testagem de sistemas de IA. Os conjuntos de dados de treino, validação e testagem deverão ter em conta, na medida do exigido face à sua finalidade prevista, as características, as funcionalidades ou os elementos que são específicos do ambiente ou do contexto geográfico, comportamental ou funcional no qual o sistema de IA será utilizado. A fim de proteger os direitos de outras pessoas da discriminação que possa resultar do enviesamento dos sistemas de IA, os fornecedores deverão poder efetuar também o tratamento de categorias especiais de dados pessoais por motivos de interesse público importante na aceção do artigo 9.º, n.º 2, alínea g), do Regulamento (UE) 2016/679 e do artigo 10.º, n.º 2, alínea g), do Regulamento (UE) 2018/1725, para assegurar o controlo, a deteção e a correção de enviesamentos em sistemas de IA de risco elevado.

(44-A) Ao aplicar os princípios referidos no artigo 5.º, n.º 1, alínea c), do Regulamento 2016/679 e no artigo 4.º, n.º 1, alínea c), do Regulamento 2018/1725, em especial o princípio da minimização dos dados, no que diz respeito aos conjuntos de dados de treino, validação e testagem ao abrigo do presente regulamento, deverá ter-se devidamente em conta o ciclo de vida completo do sistema de IA.

(45) No contexto do desenvolvimento de sistemas de IA de risco elevado, determinados intervenientes, como fornecedores, organismos notificados e outras entidades interessadas, como polos de inovação digital, instalações de teste e experimentação e investigadores, devem poder aceder e utilizar conjuntos de dados de elevada qualidade dentro das respetivas áreas de intervenção relacionadas com o presente regulamento. Os espaços comuns europeus de dados criados pela Comissão e a facilitação da partilha de dados entre empresas e com as administrações públicas por motivos de interesse público serão cruciais para conceder um acesso fiável, responsável e não discriminatório a dados de elevada qualidade para o treino, a validação e o testagem de sistemas de IA. Por exemplo, no domínio da saúde, o espaço europeu de dados de saúde facilitará o acesso não discriminatório a dados de saúde e o treino de algoritmos de inteligência artificial com base nesses conjuntos de dados, de forma segura, oportuna, transparente, fidedigna e protetora da privacidade e sob a alçada de uma governação institucional adequada. As autoridades competentes, incluindo as autoridades setoriais, que concedem ou apoiam o acesso aos dados também podem apoiar o fornecimento de dados de elevada qualidade para fins de treino, validação e testagem de sistemas de IA.

(46) Para verificar o cumprimento dos requisitos estabelecidos no presente regulamento, é essencial dispor de informações sobre o desenvolvimento dos sistemas de IA de risco elevado e sobre o seu desempenho ao longo do respetivo ciclo de vida. Tal exige a manutenção de registos e a disponibilização de documentação técnica que contenham as informações necessárias para avaliar o cumprimento, por parte do sistema de IA, dos requisitos aplicáveis. Essas informações devem incluir as características gerais, as capacidades e as limitações do sistema, os algoritmos, os dados e os processos de treino, testagem e validação utilizados, bem como documentação sobre o sistema de gestão de riscos aplicado. A documentação técnica deve estar sempre atualizada. Além disso, os fornecedores ou utilizadores deverão conservar registos gerados automaticamente pelo sistema de IA de risco elevado, incluindo, por exemplo, dados de saída, data e hora de início, entre outros, na medida em que esse sistema e os registos conexos estejam sob o seu controlo, durante um período adequado para lhes permitir cumprir as suas obrigações.

(47) Para fazer face à opacidade que pode tornar determinados sistemas de IA incompreensíveis ou demasiado complexos para as pessoas singulares, os sistemas de IA de risco elevado devem observar um certo grau de transparência. Os utilizadores devem ser capazes de interpretar o resultado do sistema e utilizá-lo de forma adequada. Como tal, os sistemas de IA de risco elevado deverão ser acompanhados de documentação pertinente e instruções de utilização e incluir informações concisas e claras, nomeadamente informações relativas a possíveis riscos para os direitos fundamentais e à discriminação de pessoas que possam ser afetadas pelo sistema à luz da sua finalidade prevista, conforme adequado. A fim de fazer com que seja mais fácil para os utilizadores compreenderem as instruções de utilização, estas deverão incluir, se for caso disso, exemplos ilustrativos.

(48) Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que permita a sua supervisão por pessoas singulares. Para o efeito, o fornecedor do sistema deve identificar medidas de supervisão humana adequadas antes da colocação no mercado ou da colocação em serviço do sistema. Em particular, se for caso disso, essas medidas devem garantir que o sistema integre restrições operacionais que não possam ser neutralizadas pelo próprio sistema e que respondam ao operador humano e que as pessoas singulares a quem foi atribuída a supervisão humana tenham as competências, a formação e a autoridade necessárias para desempenhar essa função. Tendo em conta as consequências significativas para as pessoas em caso de correspondências incorretas por determinados sistemas de identificação biométrica, é conveniente prever um requisito reforçado de supervisão humana para esses sistemas, de modo a que o utilizador não possa tomar qualquer medida ou decisão com base na identificação resultante do sistema, a menos que tal tenha sido verificado separadamente e confirmado por, pelo menos, duas pessoas singulares. Essas pessoas podem pertencer a uma ou mais entidades e incluir a pessoa que opera ou utiliza o sistema. Este requisito não deverá implicar encargos ou atrasos desnecessários e pode ser suficiente que as verificações separadas efetuadas pelas diferentes pessoas sejam automaticamente gravadas nos registos gerados pelo sistema.

(49) Os sistemas de IA de risco elevado devem ter um desempenho coerente ao longo de todo o ciclo de vida e apresentar um nível adequado de exatidão, solidez e cibersegurança, de acordo com o estado da técnica geralmente reconhecido. O nível e as métricas de exatidão devem ser comunicadas aos utilizadores.

(50) A solidez técnica é um requisito essencial dos sistemas de IA de risco elevado. Esses sistemas deverão ser resistentes a comportamentos prejudiciais ou indesejáveis que possam resultar de limitações dentro dos sistemas ou do ambiente em que os sistemas operam (por exemplo, erros, falhas, incoerências, situações inesperadas). Por conseguinte, os sistemas de IA de risco elevado deverão ser concebidos e desenvolvidos com soluções técnicas adequadas para prevenir ou minimizar esses comportamentos prejudiciais ou indesejáveis, como, por exemplo, mecanismos que permitam ao sistema interromper de forma segura o seu funcionamento (planos de segurança à prova de falhas) na presença de determinadas anomalias ou quando o funcionamento ocorre fora de certos limites predeterminados. A falta de proteção contra estes riscos pode causar problemas de segurança ou afetar negativamente os direitos fundamentais, por exemplo, devido a decisões erradas ou a resultados errados ou enviesados gerados pelo sistema de IA.

(51) A cibersegurança desempenha um papel fundamental para garantir que os sistemas de IA sejam resistentes às ações de terceiros mal-intencionados que tentam explorar as vulnerabilidades dos sistemas com o objetivo de lhes alterar a utilização, o comportamento e o desempenho ou por em causa as propriedades de segurança. Os ciberataques contra sistemas de IA podem tirar partido de ativos específicos de inteligência artificial, como os conjuntos de dados de treino (por exemplo, contaminação de dados) ou os modelos treinados (por exemplo, ataques antagónicos), ou explorar vulnerabilidades dos ativos digitais do sistema de IA ou da infraestrutura de tecnologias da informação e comunicação (TIC) subjacente. A fim de assegurar um nível de cibersegurança adequado aos riscos, os fornecedores de sistemas de IA de risco elevado devem tomar medidas adequadas, tendo ainda em devida conta a infraestrutura de TIC subjacente.

(52) No âmbito da legislação de harmonização da União, deverão ser estabelecidas regras aplicáveis à colocação no mercado, à colocação em serviço e à utilização de sistemas de IA de risco elevado coerentes com o Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho[22], que estabelece os requisitos de acreditação e fiscalização de produtos, a Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho[23], relativa a um quadro comum para a comercialização de produtos, e o Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho[24], relativo à fiscalização do mercado e à conformidade dos produtos (a seguir designados conjuntamente por "novo quadro legislativo [para a comercialização de produtos]").

(52-A) Em consonância com os princípios do novo quadro legislativo, deverão ser estabelecidas obrigações específicas aplicáveis aos operadores pertinentes da cadeia de valor da IA, de modo que garanta a segurança jurídica e facilite a conformidade com o presente regulamento. Em determinadas situações, esses operadores podem desempenhar mais do que uma função ao mesmo tempo, pelo que deverão cumprir cumulativamente todas as obrigações relevantes associadas a essas funções. Por exemplo, um operador pode atuar simultaneamente como distribuidor e importador.

(53) É apropriado que uma pessoa singular ou coletiva específica, identificada como "fornecedor", assuma a responsabilidade pela colocação no mercado ou pela colocação em serviço de um sistema de IA de risco elevado, independentemente de ser ou não a pessoa que concebeu ou desenvolveu o sistema.

---

22 Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).

23 Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativa a um quadro comum para a comercialização de produtos, e que revoga a Decisão 93/465/CEE (JO L 218 de 13.8.2008, p. 82).

24 Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à fiscalização do mercado e à conformidade dos produtos e que altera a Diretiva 2004/42/CE e os Regulamentos (CE) n.º 765/2008 e (UE) n.º 305/2011 (Texto relevante para efeitos do EEE) (JO L 169 de 25.6.2019, pp. 1-44).

(54) O fornecedor deve introduzir um sistema de gestão da qualidade sólido, garantir a realização do procedimento de avaliação da conformidade exigido, elaborar a documentação pertinente e estabelecer um sistema de acompanhamento pós-comercialização capaz. As autoridades públicas que colocam em serviço sistemas de IA de risco elevado para sua própria utilização podem adotar e aplicar as regras relativas ao sistema de gestão da qualidade no âmbito do sistema de gestão da qualidade adotado a nível nacional ou regional, consoante o caso, tendo em conta as especificidades do setor e as competências e a organização da autoridade pública em causa.

(54-A) A fim de garantir a segurança jurídica, é necessário tornar claro que, em determinadas condições específicas, as pessoas singulares ou coletivas deverão ser consideradas como fornecedores de um novo sistema de IA de risco elevado e, por conseguinte, deverão assumir todas as obrigações pertinentes. Por exemplo, será esse o caso se uma pessoa puser o seu nome ou marca num sistema de IA de risco elevado já colocado no mercado ou colocado em serviço, ou se alterar a finalidade prevista de um sistema de IA que não seja de risco elevado e já tenha sido colocado no mercado ou colocado em serviço de uma forma que torne esse sistema alterado num sistema de IA de risco elevado. Estas disposições deverão aplicar-se sem prejuízo das disposições mais específicas estabelecidas em determinada legislação setorial do novo quadro legislativo, a qual deverá ser aplicada conjuntamente com o presente regulamento. Por exemplo, o artigo 16.º, n.º 2, do Regulamento (UE) 2017/745, que estabelece que determinadas alterações não são consideradas alterações de um dispositivo suscetíveis de afetar a sua conformidade com os requisitos aplicáveis, deverá continuar a aplicar-se aos sistemas de IA de risco elevado que sejam dispositivos médicos na aceção do referido regulamento.

(55) Caso um sistema de IA de risco elevado que é um componente de segurança de um produto abrangido por legislação setorial do novo quadro legislativo não seja colocado no mercado ou em serviço de forma independente desse produto, o fabricante do produto, conforme definido no correspondente ato do novo quadro legislativo, deverá cumprir as obrigações dos fornecedores estabelecidas no presente regulamento e assegurar que o sistema de IA integrado no produto final cumpre os requisitos do presente regulamento.

(56) Para permitir a execução do presente regulamento e criar condições de concorrência equitativas para os operadores, tendo ainda em conta as diferentes formas de disponibilização de produtos digitais, é importante assegurar que, em qualquer circunstância, uma pessoa estabelecida na União possa fornecer às autoridades todas as informações necessárias sobre a conformidade de um sistema de IA. Como tal, antes de disponibilizarem os seus sistemas de IA na União, caso não seja possível identificar um importador, os fornecedores estabelecidos fora da União devem, através de mandato escrito, designar um mandatário estabelecido na União.

(56-A) No atinente aos fornecedores que não se encontram estabelecidos na União, o mandatário desempenha um papel central ao garantir a conformidade dos sistemas de IA de risco elevado colocados no mercado ou colocados em serviço na União por esses fornecedores e ao atuar como a sua pessoa de contacto estabelecida na União. Dado esse papel central, e a fim de assegurar que a responsabilidade é assumida para efeitos de execução do presente regulamento, é adequado tornar o mandatário solidariamente responsável com o fornecedor pelos sistemas de IA de risco elevado defeituosos. A responsabilidade do mandatário prevista no presente regulamento não prejudica o disposto na Diretiva 85/374/CEE relativa à responsabilidade decorrente dos produtos defeituosos.

(57) [suprimido]

(58) Dada a natureza dos sistemas de IA e os riscos para a segurança e os direitos fundamentais possivelmente associados à sua utilização, nomeadamente no que respeita à necessidade de assegurar um controlo adequado do desempenho de um sistema de IA num cenário real, é apropriado determinar responsabilidades específicas para os utilizadores. Em particular, os utilizadores devem utilizar os sistemas de IA de risco elevado de acordo com as instruções de utilização e devem ser equacionadas outras obrigações relativas ao controlo do funcionamento dos sistemas de IA e à manutenção de registos, se for caso disso. Essas obrigações não deverão prejudicar outras obrigações dos utilizadores em relação a sistemas de IA de risco elevado ao abrigo do direito da União ou do direito nacional, e não deverão aplicar-se se o sistema for utilizado no âmbito de uma atividade pessoal de caráter não profissional.

(58-A) Importa tornar claro que o presente regulamento não afeta as obrigações dos fornecedores e utilizadores de sistemas de IA no seu papel de responsáveis pelo tratamento de dados ou de subcontratantes decorrentes do direito da União em matéria de proteção de dados pessoais, na medida em que a conceção, o desenvolvimento ou a utilização de sistemas de IA envolva o tratamento de dados pessoais. É igualmente conveniente clarificar que os titulares de dados continuam a usufruir de todos os direitos e garantias que lhes são conferidos por esse direito da União, incluindo os direitos relacionados com as decisões individuais exclusivamente automatizadas, nomeadamente a definição de perfis. As regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA estabelecidas no presente regulamento deverão facilitar a aplicação efetiva e permitir o exercício dos direitos dos titulares de dados e de outras vias de recurso garantidas pelo direito da União em matéria de proteção de dados pessoais e de outros direitos fundamentais.

(59) [suprimido]

(60) [suprimido]

(61) A normalização deverá desempenhar um papel fundamental, disponibilizando aos fornecedores soluções técnicas que assegurem o cumprimento do presente regulamento, em conformidade com o estado da técnica. O cumprimento de normas harmonizadas conforme definido no Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho[25], que normalmente se espera que reflitam o estado da técnica, deverá constituir um meio de os fornecedores demonstrarem a conformidade com os requisitos do presente regulamento. No entanto, na ausência de referências pertinentes a normas harmonizadas, a Comissão deverá poder estabelecer, através de atos de execução, especificações comuns para determinados requisitos ao abrigo do presente regulamento como solução de recurso excecional para facilitar a obrigação do fornecedor de cumprir os requisitos do presente regulamento, caso o processo de normalização esteja bloqueado ou caso haja atrasos no estabelecimento de uma norma harmonizada adequada. Se esse atraso se dever à complexidade técnica da norma em questão, a Comissão deverá tomar esse facto em consideração antes de ponderar o estabelecimento de especificações comuns. A participação adequada das pequenas e médias empresas na elaboração de normas de apoio à aplicação do presente regulamento é essencial para promover a inovação e a competitividade no domínio da inteligência artificial na União. Essa participação deverá ser assegurada de forma adequada, em conformidade com os artigos 5.º e 6.º do Regulamento (UE) n.º 1025/2012.

[25] Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

(61-A) É conveniente que, sem prejuízo da utilização de normas harmonizadas e especificações comuns, os fornecedores beneficiem de uma presunção de conformidade com o requisito pertinente em matéria de dados quando o seu sistema de IA de risco elevado tiver sido treinado e testado em dados que reflitam o contexto geográfico, comportamental ou funcional específico em que o sistema de IA se destina a ser utilizado. Do mesmo modo, em conformidade com o artigo 54.º, n.º 3, do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, deverá presumir-se que os sistemas de IA de risco elevado que tenham sido certificados ou para os quais tenha sido emitida uma declaração de conformidade no âmbito de um sistema de certificação de cibersegurança estabelecido nos termos desse regulamento, e cujas referências tenham sido publicadas no Jornal Oficial da União Europeia, estão em conformidade com o requisito de cibersegurança do presente regulamento. Tal não prejudica a natureza voluntária desse sistema de certificação de cibersegurança.

(62) A fim de assegurar um nível elevado de fiabilidade dos sistemas de IA de risco elevado, estes devem ser sujeitos a uma avaliação da conformidade antes de serem colocados no mercado ou em serviço.

(63) Para minimizar os encargos impostos aos operadores e evitar possíveis duplicações, é apropriado que, no caso dos sistemas de IA de risco elevado relacionados com produtos abrangidos por legislação de harmonização da União na sequência da abordagem do novo quadro legislativo, o cumprimento dos requisitos do presente regulamento por parte desses sistemas de IA seja aferido no âmbito da avaliação da conformidade já prevista nessa legislação. Como tal, a aplicabilidade dos requisitos do presente regulamento não deve afetar a lógica, a metodologia ou a estrutura geral específicas da avaliação da conformidade realizada nos termos do correspondente ato do novo quadro legislativo. Esta abordagem encontra-se refletida na íntegra na interligação entre o presente regulamento e o [Regulamento Máquinas]. Embora os riscos de segurança dos sistemas de IA que garantem funções de segurança nas máquinas sejam tratados nos requisitos do presente regulamento, determinados requisitos específicos do [Regulamento Máquinas] assegurarão a integração segura de sistemas de IA nas máquinas em geral, de modo que não ponha em causa a segurança das máquinas no seu todo. O [Regulamento Máquinas] aplica a mesma definição de sistema de IA do presente regulamento. No que diz respeito aos sistemas de IA de risco elevado relacionados com produtos abrangidos pelos Regulamentos (UE) 2017/745 e (UE) 2017/746 relativos aos dispositivos médicos, a aplicabilidade dos requisitos do presente regulamento não deverá prejudicar e deverá ter em conta a lógica de gestão dos riscos e a avaliação da relação benefício-risco realizada ao abrigo do quadro relativo aos dispositivos médicos.

(64) Dada a experiência mais vasta dos certificadores de pré-comercialização profissionais no domínio da segurança dos produtos e a diferente natureza dos riscos inerentes, é apropriado limitar, pelo menos numa fase inicial da aplicação do presente regulamento, o âmbito da avaliação da conformidade por terceiros aos sistemas de IA de risco elevado que não estejam relacionados com produtos. Como tal, a avaliação da conformidade desses sistemas deve ser realizada, regra geral, pelo fornecedor sob a sua própria responsabilidade, com a exceção única dos sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância de pessoas, cuja avaliação da conformidade, contanto que os sistemas em causa não sejam proibidos, deve contar com a participação de um organismo notificado.

(65) Para efeitos de avaliação da conformidade por terceiros de sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância de pessoas, os organismos notificados deverão ser notificados pelas autoridades nacionais competentes no âmbito do presente regulamento, desde que cumpram uma série de requisitos, nomeadamente em termos de independência, competência e ausência de conflitos de interesse. A notificação desses organismos deverá ser enviada pelas autoridades nacionais competentes à Comissão e aos outros Estados-Membros por meio do instrumento de notificação eletrónica desenvolvido e gerido pela Comissão nos termos do artigo R23 da Decisão n.º 768/2008/CE.

(66) Em consonância com a noção comummente estabelecida de modificação substancial de produtos regulamentados pela legislação de harmonização da União, é apropriado que, sempre que ocorra uma alteração que possa afetar a conformidade de um sistema de IA de risco elevado com o presente Regulamento (por exemplo, alteração do sistema operativo ou da arquitetura do software), ou sempre que a finalidade prevista do sistema se altere, esse sistema de IA deverá ser considerado um novo sistema de IA que deve ser submetido a uma nova avaliação da conformidade. No entanto, as alterações que ocorrem no algoritmo e no desempenho dos sistemas de IA que continuam a "aprender" depois de terem sido colocados no mercado ou em serviço (ou seja, que adaptam automaticamente o modo de funcionamento) não deverão constituir uma modificação substancial, desde que tenham sido predeterminadas pelo fornecedor e examinadas aquando da avaliação da conformidade.

(67) Para que possam circular livremente dentro do mercado interno, os sistemas de IA de risco elevado devem apresentar a marcação CE para indicar o cumprimento do presente regulamento. Os Estados-Membros não podem criar obstáculos injustificados à colocação no mercado ou à colocação em serviço de sistemas de IA de risco elevado que cumpram os requisitos previstos no presente regulamento e apresentem a marcação CE.

(68) Em certas condições, uma disponibilização rápida de tecnologias inovadoras pode ser crucial para a saúde e a segurança das pessoas e da sociedade em geral. Como tal, é apropriado que, por razões excecionais de segurança pública ou proteção da vida e da saúde das pessoas singulares e de proteção da propriedade industrial e comercial, os Estados-Membros possam autorizar a colocação no mercado ou a colocação em serviço de sistemas de IA que não foram objeto de uma avaliação da conformidade.

(69) Para facilitar o trabalho da Comissão e dos Estados-Membros no domínio da inteligência artificial, bem como aumentar a transparência para o público, os fornecedores de sistemas de IA de risco elevado que não os relacionados com produtos abrangidos pelo âmbito da atual legislação de harmonização da União deverão ser obrigados a registarem-se a si mesmos e a registar as informações sobre esses sistemas de IA de risco elevado numa base de dados da UE que será criada e gerida pela Comissão. Antes de utilizarem um dos sistemas de IA de risco elevado enumerados no anexo III, os utilizadores de sistemas de IA de risco elevado que sejam autoridades, agências ou organismos públicos – com exceção das autoridades competentes em matéria de manutenção da ordem pública, controlo das fronteiras, imigração ou asilo, e das autoridades que utilizam sistemas de IA de risco elevado no domínio das infraestruturas críticas – deverão também registar-se nessa base de dados e selecionar o sistema que tencionam utilizar. A Comissão deverá ser o responsável pelo tratamento dessa base de dados, nos termos do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho[26]. Para assegurar que a base de dados esteja plenamente operacional à data de implantação, o procedimento para a criação da base de dados deve incluir a elaboração de especificações funcionais pela Comissão e um relatório de auditoria independente.

26 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

(70) Determinados sistemas de IA concebidos para interagir com pessoas singulares ou para criar conteúdos podem representar riscos específicos de usurpação de identidade ou fraude, independentemente de serem considerados de risco elevado ou não. Como tal, em certas circunstâncias, a utilização destes sistemas deve ser sujeita a obrigações de transparência específicas sem prejudicar os requisitos e as obrigações aplicáveis aos sistemas de IA de risco elevado. Em particular, as pessoas singulares deverão ser notificadas de que estão a interagir com um sistema de IA, salvo se tal se revelar óbvio do ponto de vista de uma pessoa singular razoavelmente informada, atenta e advertida, tendo em conta as circunstâncias e o contexto de utilização. Ao aplicar essa obrigação, as características das pessoas pertencentes a grupos vulneráveis devido à sua idade ou deficiência deverão ser tidas em conta na medida em que o sistema de IA também se destine a interagir com esses grupos. Além disso, as pessoas singulares deverão ser notificadas quando forem expostas a sistemas que, através do tratamento dos seus dados biométricos, possam identificar ou inferir as emoções ou intenções dessas pessoas ou atribuí-las a categorias específicas. Essas categorias específicas podem dizer respeito a aspetos como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, traços de personalidade, origem étnica, preferências e interesses pessoais ou outros aspetos, como a orientação sexual ou política. Essas informações e notificações devem ser fornecidas em formatos acessíveis a pessoas com deficiência. Além disso, os utilizadores que recorrem a um sistema de IA para gerar ou manipular conteúdos de imagem, áudio ou vídeo que sejam consideravelmente semelhantes a pessoas, locais ou acontecimentos reais e que, falsamente, pareçam ser autênticos a outrem devem divulgar que os conteúdos foram criados de forma artificial ou manipulados, identificando como tal o resultado da inteligência artificial e divulgando a sua origem artificial. O cumprimento das obrigações de informação acima referidas não deverá ser interpretado como indicando que a utilização do sistema ou os seus resultados é lícita ao abrigo do presente regulamento ou de outra legislação da União e dos Estados-Membros e não deverá prejudicar outras obrigações de transparência para com os utilizadores de sistemas de IA estabelecidas na legislação da União ou nacional. Além disso, também não deverá ser interpretado como indicando que a utilização do sistema ou dos seus resultados entrava o direito à liberdade de expressão e o direito à liberdade das artes e das ciências consagrados na Carta dos Direitos Fundamentais da UE, em especial se os conteúdos fizerem parte de uma obra ou programa manifestamente criativos, satíricos, artísticos ou fictícios, sob reserva de garantias adequadas para os direitos e liberdades de terceiros.

(71) A inteligência artificial é uma família de tecnologias em rápida evolução que exige novas formas de supervisão regulamentar e um espaço seguro para a experimentação, garantindo ao mesmo tempo uma inovação responsável e a integração de salvaguardas e medidas de atenuação dos riscos adequadas. Para assegurar um quadro jurídico propício à inovação, preparado para o futuro e resistente a perturbações, as autoridades nacionais competentes de um ou vários Estados-Membros devem ser incentivadas a criar ambientes de testagem da regulamentação da inteligência artificial que facilitem o desenvolvimento e a testagem de sistemas de IA inovadores sob uma supervisão regulamentar rigorosa, antes que estes sistemas sejam colocados no mercado ou em serviço.

(72) Os objetivos dos ambientes de testagem da regulamentação da IA deverão centrar-se em fomentar a inovação no domínio da IA, mediante a criação de um ambiente controlado de experimentação e testagem na fase de desenvolvimento e pré-comercialização, com vista a assegurar que os sistemas de IA inovadores cumprem o presente regulamento e outra legislação aplicável dos Estados-Membros e da União; melhorar a supervisão e a compreensão, por parte das autoridades competentes, das oportunidades, dos riscos emergentes e dos impactos da utilização da inteligência artificial; e acelerar o acesso aos mercados, nomeadamente por via da eliminação dos entraves para as pequenas e médias empresas (PME), incluindo as empresas em fase de arranque. A participação nos ambientes de testagem da regulamentação da IA deverá centrar-se em questões que levantam incerteza jurídica para os fornecedores e potenciais fornecedores inovarem, fazerem experiências com a IA na União e contribuírem para uma aprendizagem regulamentar baseada em dados concretos. A supervisão dos sistemas de IA nos ambientes de testagem da regulamentação da IA deverá, por conseguinte, abranger o seu desenvolvimento, treino, testagem e validação antes de os sistemas serem colocados no mercado ou colocados em serviço, bem como a noção e a ocorrência de modificação substancial que possa exigir um novo procedimento de avaliação da conformidade. Se for caso disso, as autoridades nacionais competentes que criam ambientes de testagem da regulamentação da IA deverão cooperar com outras autoridades pertinentes, incluindo as que supervisionam a proteção dos direitos fundamentais, e podem permitir a participação de outros intervenientes no ecossistema de IA, tais como organizações de normalização, organismos notificados, laboratórios e instalações de ensaio e experimentação, polos de inovação e organizações pertinentes das partes interessadas e da sociedade civil, quer nacionais quer europeus. Para assegurar uma aplicação uniforme em toda a União e economias de escala, é apropriado criar regras comuns para a implantação dos ambientes de testagem da regulamentação e um quadro para a cooperação entre as autoridades competentes envolvidas na supervisão desses ambientes. Os ambientes de testagem da regulamentação da IA criados ao abrigo do presente regulamento não deverão prejudicar outra legislação que permita a criação de outros ambientes de testagem destinados a assegurar o cumprimento de legislação que não a do presente regulamento. Se for caso disso, as autoridades competentes responsáveis por esses outros ambientes de testagem da regulamentação deverão ter em conta os benefícios da utilização desses ambientes de testagem também com o objetivo de assegurar a conformidade dos sistemas de IA com o presente regulamento. Mediante acordo entre as autoridades nacionais competentes e os participantes no ambiente de testagem da regulamentação da IA, a testagem em condições reais também pode ser efetuada e supervisionada no âmbito do ambiente de testagem da regulamentação da IA.

(-72-A) O presente regulamento deverá estabelecer o fundamento jurídico para a utilização, pelos participantes no ambiente de testagem da regulamentação da IA, de dados pessoais recolhidos para outras finalidades com vista ao desenvolvimento de determinados sistemas de IA por motivos de interesse público no âmbito do ambiente de testagem da regulamentação da IA, em conformidade com os artigos 6.º, n.º 4, e 9.º, n.º 2, alínea g),do Regulamento (UE) 2016/679 e dos artigos 5.º e 10.º do Regulamento (UE) 2018/1725, e sem prejuízo dos artigos 4.º, n.º 2, e 10.º da Diretiva (UE) 2016/680. Todas as outras obrigações dos responsáveis pelo tratamento de dados e todos os outros direitos dos titulares dos dados ao abrigo do Regulamento (UE) 2016/679, do Regulamento (UE) 2018/1725 e da Diretiva (UE) 2016/680 continuam a ser aplicáveis. Em especial, o presente regulamento não deverá constituir uma base jurídica na aceção do artigo 22.º, n.º 2, alínea b), do Regulamento (UE) 2016/679 e do artigo 24.º, n.º 2, alínea b), do Regulamento (UE) 2018/1725. Os participantes no ambiente de testagem devem assegurar salvaguardas adequadas e cooperar com as autoridades competentes, nomeadamente seguindo as suas orientações e atuando de forma célere e de boa-fé para atenuar eventuais riscos elevados para a segurança e os direitos fundamentais que possam revelar-se durante o desenvolvimento e a experimentação no ambiente de testagem. A conduta dos participantes no ambiente de testagem deve ser tida em conta quando as autoridades competentes decidirem sobre a aplicação de uma coima, nos termos do artigo 83.º, n.º 2, do Regulamento (UE) 2016/679 e do artigo 57.º da Diretiva (UE) 2016/680.

(72-A) A fim de acelerar o processo de desenvolvimento e colocação no mercado dos sistemas de IA de risco elevado enumerados no anexo III, é importante que os fornecedores ou potenciais fornecedores desses sistemas possam também beneficiar de um regime específico para testar esses sistemas em condições reais, sem participarem num ambiente de testagem da regulamentação da IA. Contudo, nesses casos, e tendo em conta as possíveis consequências desses testes para as pessoas singulares, deverá garantir-se que o regulamento introduz garantias e condições adequadas e suficientes para os fornecedores ou potenciais fornecedores. Essas garantias deverão incluir, nomeadamente, o pedido de consentimento informado às pessoas singulares para participarem na testagem em condições reais, com exceção das autoridades policiais nos casos em que a obtenção do consentimento informado impeça o sistema de IA de ser testado. O consentimento das pessoas singulares para participar nessa testagem ao abrigo do presente regulamento é distinto e sem prejuízo do consentimento dos titulares dos dados para o tratamento dos seus dados pessoais ao abrigo da legislação aplicável em matéria de proteção de dados.

(73) A fim de promover e proteger a inovação, é importante ter em especial atenção os interesses dos fornecedores e utilizadores de sistemas de IA que são PME. Para esse efeito, os Estados-Membros devem desenvolver iniciativas dirigidas a esses operadores, incluindo ações de sensibilização e comunicação de informações. Além disso, os interesses e as necessidades específicas dos fornecedores que são PME deverão ser tidos em conta quando os organismos notificados fixam as taxas a pagar pela avaliação da conformidade. Os custos de tradução associados à documentação obrigatória e à comunicação com as autoridades podem constituir um custo substancial para os fornecedores e outros operadores, nomeadamente para os fornecedores de menor dimensão. Os Estados-Membros podem eventualmente assegurar que uma das línguas por si determinadas e aceites para a elaboração de documentação pelos fornecedores e a comunicação com os operadores seja uma língua amplamente compreendida pelo maior número possível de utilizadores transfronteiras.

(73-A) A fim de promover e proteger a inovação, a plataforma IA a pedido, todos os programas e projetos de financiamento pertinentes da UE, como o Programa Europa Digital e o Horizonte Europa, executados pela Comissão e pelos Estados-Membros a nível nacional ou da UE, deverão contribuir para a consecução dos objetivos do presente regulamento.

(74) Em particular, para minimizar os riscos para a aplicação resultantes da falta de conhecimentos e competências especializadas no mercado, bem como facilitar o cumprimento, por parte dos fornecedores, nomeadamente as PME, e dos organismos notificados, das obrigações que lhes são impostas pelo presente regulamento, a plataforma IA a pedido, os polos europeus de inovação digital e as instalações de ensaio e experimentação criadas pela Comissão e pelos Estados-Membros a nível nacional ou europeu podem eventualmente contribuir para a aplicação do presente regulamento. No âmbito da respetiva missão e domínios de competência, estas entidades podem prestar apoio técnico e científico aos fornecedores e aos organismos notificados.

(74-A) Além disso, a fim de assegurar a proporcionalidade tendo em conta a dimensão muito reduzida de alguns operadores no que diz respeito aos custos da inovação, é adequado isentar as microempresas das obrigações mais onerosas, como o estabelecimento de um sistema de gestão da qualidade que reduza os encargos administrativos e os custos para essas empresas sem afetar o nível de proteção e a necessidade de cumprir os requisitos aplicáveis aos sistemas de IA de risco elevado.

(75) É apropriado que a Comissão facilite, tanto quanto possível, o acesso a instalações de teste e experimentação aos organismos, grupos ou laboratórios criados ou acreditados nos termos da legislação de harmonização da União pertinente e que desempenham funções no contexto da avaliação da conformidade dos produtos ou dispositivos abrangidos por essa legislação de harmonização da União. Tal é, nomeadamente, o caso dos painéis de peritos, dos laboratórios especializados e dos laboratórios de referência no domínio dos dispositivos médicos, referidos nos Regulamentos (UE) 2017/745 e (UE) 2017/746.

(76) A fim de facilitar uma aplicação simples, eficaz e harmoniosa do presente regulamento, deverá ser criado um Comité Europeu para a Inteligência Artificial. O Comité deverá refletir os vários interesses do ecossistema de IA e ser composto por representantes dos Estados-Membros. A fim de assegurar a participação das partes interessadas pertinentes, deverá ser criado um subgrupo permanente do Comité. O Comité deverá ser responsável por uma série de funções consultivas, nomeadamente a emissão de pareceres, recomendações, conselhos ou o contributo para orientações em questões relacionadas com a aplicação do presente regulamento, inclusive no tocante a questões de execução, especificações técnicas ou normas existentes relativas aos requisitos indicados no presente regulamento, e a prestação de aconselhamento à Comissão a aos Estados-Membros e respetivas autoridades nacionais competentes sobre questões específicas relacionadas com a inteligência artificial. A fim de dar alguma flexibilidade aos Estados-Membros na designação dos seus representantes no Comité para a Inteligência Artificial, esses representantes podem ser quaisquer pessoas pertencentes a entidades públicas que devem ter as competências e os poderes pertinentes para facilitar a coordenação a nível nacional e contribuir para o desempenho das funções do Comité. O Comité deverá criar dois subgrupos permanentes a fim de proporcionar uma plataforma de cooperação e intercâmbio entre as autoridades de fiscalização do mercado e as autoridades notificadoras sobre questões relacionadas, respetivamente, com a fiscalização do mercado e os organismos notificados. O subgrupo permanente para a fiscalização do mercado deverá atuar como grupo de cooperação administrativa (ADCO) para efeitos do presente regulamento, na aceção do artigo 30.º do Regulamento (UE) 2019/1020. Em consonância com o papel e as atribuições da Comissão nos termos do artigo 33.º do Regulamento (UE) 2019/1020, a Comissão deverá apoiar as atividades do subgrupo permanente para a fiscalização do mercado, realizando avaliações ou estudos de mercado, nomeadamente com vista a identificar aspetos do presente regulamento que exijam uma coordenação específica e urgente entre as autoridades de fiscalização do mercado. O Comité pode constituir outros subgrupos permanentes ou temporários consoante adequado para efeitos da análise de questões específicas. O Comité deverá também cooperar, se for caso disso, com os organismos, grupos de peritos e redes pertinentes da UE ativos no contexto da legislação pertinente da UE, incluindo, em especial, os que operam ao abrigo da regulamentação pertinente da UE em matéria de dados, produtos e serviços digitais.

(76-A) A Comissão deverá apoiar ativamente os Estados-Membros e os operadores na aplicação e execução do presente regulamento. A este respeito, deverá elaborar orientações sobre temas específicos destinados a facilitar a aplicação do presente regulamento, prestando especial atenção às necessidades das PME e das empresas em fase de arranque dos setores mais suscetíveis de serem afetados. A fim de apoiar a execução adequada e as capacidades dos Estados-Membros, deverão ser criadas e disponibilizadas aos Estados-Membros instalações de ensaio da União no domínio da IA, bem como um grupo de peritos competentes.

(77) Os Estados-Membros desempenham um papel fundamental na aplicação e execução do presente regulamento. Nesse sentido, cada Estado-Membro deve designar uma ou várias autoridades nacionais competentes para efeitos de supervisão da aplicação e execução do presente regulamento. Os Estados-Membros podem decidir nomear qualquer tipo de entidade pública para desempenhar as funções das autoridades nacionais competentes na aceção do presente regulamento, de acordo com as suas características e necessidades específicas em matéria de organização nacional.

(78) Para assegurar que os fornecedores de sistemas de IA de risco elevado possam aproveitar a experiência adquirida na utilização de sistemas de IA de risco elevado para melhorarem os seus sistemas e o processo de conceção e desenvolvimento ou possam adotar possíveis medidas corretivas em tempo útil, todos os fornecedores devem dispor de um sistema de acompanhamento pós-comercialização. Este sistema também é fundamental para assegurar uma resolução mais eficaz e atempada dos eventuais riscos decorrentes dos sistemas de IA que continuam a "aprender" depois de terem sido colocados no mercado ou em serviço. Neste contexto, os fornecedores deverão ainda ser obrigados a introduzir um sistema para comunicar às autoridades competentes quaisquer incidentes graves resultantes da utilização dos sistemas de IA que fornecem.

(79) Para assegurar uma execução adequada e eficaz dos requisitos e das obrigações estabelecidas no presente regulamento, que faz parte da legislação de harmonização da União, o sistema de fiscalização do mercado e de conformidade dos produtos estabelecido no Regulamento (UE) 2019/1020 deve ser aplicado na íntegra. As autoridades de fiscalização do mercado designadas nos termos do presente regulamento deverão dispor de todos os poderes de execução ao abrigo do presente regulamento e do Regulamento (UE) 2019/1020 e deverão exercer os seus poderes e desempenhar as suas funções de forma independente, imparcial e objetiva. Embora a maioria dos sistemas de IA não esteja sujeita a requisitos e obrigações específicos ao abrigo do presente regulamento, as autoridades de fiscalização do mercado podem tomar medidas em relação a todos os sistemas de IA quando estes apresentem riscos em conformidade com o presente regulamento. Dada a natureza específica das instituições, órgãos e organismos da União abrangidos pelo âmbito de aplicação do presente regulamento, é conveniente designar a Autoridade Europeia para a Proteção de Dados como autoridade de fiscalização do mercado competente relativamente a essas instituições, órgãos e organismos. Tal não deverá prejudicar a designação das autoridades nacionais competentes pelos Estados-Membros. As atividades de fiscalização do mercado não deverão afetar a capacidade das entidades supervisionadas de desempenharem as suas funções de forma independente, quando essa independência for exigida pelo direito da União.

(79-A) O presente regulamento não prejudica as competências, as atribuições, os poderes nem a independência das autoridades ou organismos públicos nacionais competentes que supervisionam a aplicação do direito da União que protege direitos fundamentais, incluindo os organismos de promoção da igualdade e as autoridades de proteção de dados. Quando tal for necessário ao cumprimento do seu mandato, essas autoridades ou organismos públicos nacionais deverão também ter acesso à documentação elaborada por força do presente regulamento. Deverá ser estabelecido um procedimento de salvaguarda específico para assegurar uma aplicação adequada e atempada dos sistemas de IA que apresentem riscos para a saúde, a segurança e os direitos fundamentais. O procedimento aplicável a esses sistemas de IA que apresentam riscos deverá ser aplicado aos sistemas de IA de risco elevado que apresentem riscos, aos sistemas proibidos que tenham sido colocados no mercado, colocados em serviço ou utilizados em violação das práticas proibidas estabelecidas no presente regulamento e aos sistemas de IA que tenham sido disponibilizados em violação dos requisitos de transparência estabelecidos no presente regulamento e que apresentem riscos.

(80) A legislação da União em matéria de serviços financeiros inclui regras e requisitos relativos à governação interna e à gestão dos riscos aplicáveis às instituições financeiras regulamentadas durante a prestação desses serviços, incluindo quando estas utilizam sistemas de IA. Para assegurar a coerência na aplicação e na execução das obrigações previstas no presente regulamento e das regras e requisitos da legislação da União aplicáveis aos serviços financeiros, as autoridades responsáveis pela supervisão e execução da legislação no domínio dos serviços financeiros deverão ser designadas autoridades competentes para efeitos de supervisão da aplicação do presente regulamento, incluindo o exercício de funções de fiscalização do mercado, no que diz respeito aos sistemas de IA fornecidos ou utilizados por instituições financeiras regulamentadas e supervisionadas, salvo se os Estados-Membros decidirem designar outra autoridade para desempenhar essas funções de fiscalização do mercado. Essas autoridades competentes deverão dispor de todos os poderes ao abrigo do presente regulamento e do Regulamento (UE) 2019/1020 relativo à fiscalização do mercado para fazer cumprir os requisitos e obrigações do presente regulamento, incluindo poderes para levar a cabo as nossas atividades de fiscalização do mercado ex post que possam ser integradas, se for caso disso, nos seus mecanismos e procedimentos de supervisão existentes ao abrigo da legislação pertinente da União em matéria de serviços financeiros. É apropriado definir que, ao atuarem como autoridades de fiscalização do mercado ao abrigo do presente regulamento, as autoridades nacionais responsáveis por supervisionar as instituições de crédito regulamentadas pela Diretiva 2013/36/UE, que participam no Mecanismo Único de Supervisão (MUS) estabelecido pelo Regulamento (CE) n.º 1024/2013 do Conselho, deverão comunicar sem demora ao Banco Central Europeu todas as informações identificadas no âmbito das suas atividades de fiscalização do mercado que possam ser de interesse potencial para as atribuições de supervisão prudencial do Banco Central Europeu especificadas nesse regulamento. A fim de reforçar a coerência entre o presente regulamento e as regras aplicáveis às instituições de crédito regulamentadas pela Diretiva 2013/36/UE do Parlamento Europeu e do Conselho[27], também é apropriado integrar algumas das obrigações processuais dos fornecedores relativas à gestão de riscos, ao acompanhamento pós-comercialização e à documentação nas obrigações e procedimentos em vigor por força da mesma diretiva. No intuito de evitar sobreposições, também devem ser previstas derrogações limitadas no respeitante ao sistema de gestão da qualidade dos fornecedores e à obrigação de controlo imposta aos utilizadores de sistemas de IA de risco elevado, contanto que tal se aplique a instituições de crédito regulamentadas pela Diretiva 2013/36/UE. Deverá aplicar-se o mesmo regime às empresas de seguros e de resseguros e às sociedades gestoras de

[27] Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).

participações no setor dos seguros nos termos da Diretiva 2009/138/CE (Solvência II), aos mediadores de seguros ao abrigo da Diretiva (UE) 2016/97 e a outros tipos de instituições financeiras sujeitas a requisitos em matéria governação, mecanismos ou processos internos estabelecidos nos termos da legislação pertinente da União em matéria de serviços financeiros, a fim de assegurar a coerência e a igualdade de tratamento no setor financeiro.

(81) O desenvolvimento de outros sistemas de IA, que não sejam sistemas de IA de risco elevado, de acordo com os requisitos do presente regulamento pode conduzir a uma maior utilização de inteligência artificial fiável na União. Os fornecedores de sistemas de IA que não são de risco elevado deverão ser incentivados a criar códigos de conduta que visem promover a aplicação voluntária dos requisitos aplicáveis aos sistemas de IA de risco elevado, adaptados à finalidade prevista dos sistemas e ao menor risco envolvido. Os fornecedores devem ainda ser incentivados a aplicar voluntariamente requisitos adicionais relacionados, por exemplo, com a sustentabilidade ambiental, a acessibilidade das pessoas com deficiência, a participação das partes interessadas na conceção e no desenvolvimento de sistemas de IA e a diversidade das equipas de desenvolvimento. A Comissão pode desenvolver iniciativas, incluindo de natureza setorial, para facilitar a redução de obstáculos técnicos que impeçam o intercâmbio transfronteiras de dados para o desenvolvimento da inteligência artificial, incluindo em matéria de infraestruturas de acesso aos dados e de interoperabilidade semântica e técnica de diferentes tipos de dados.

(82) Não obstante, é importante que os sistemas de IA relacionados com produtos que não são de risco elevado, nos termos do presente regulamento, e que, como tal, não são obrigados a cumprir os requisitos do mesmo, sejam seguros quando são colocados no mercado ou em serviço. A fim de contribuir para alcançar esse objetivo, a Diretiva 2001/95/CE do Parlamento Europeu e do Conselho[28] será aplicada como uma rede de segurança.

(83) Para assegurar uma cooperação de confiança e construtiva entre as autoridades competentes a nível da União e nacional, todas as partes envolvidas na aplicação do presente regulamento deverão respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções, em conformidade com a legislação da União ou nacional.

---

28 Diretiva 2001/95/CE do Parlamento Europeu e do Conselho, de 3 de dezembro de 2001, relativa à segurança geral dos produtos (JO L 11 de 15.1.2002, p. 4).

(84) Os Estados-Membros devem tomar todas as medidas necessárias para assegurar a aplicação das disposições do presente regulamento, inclusive estabelecendo sanções efetivas, proporcionadas e dissuasivas aplicáveis à sua violação, e no respeito do princípio *ne bis in idem*. No caso de determinadas violações específicas, os Estados-Membros devem ter em conta as margens e os critérios estabelecidos no presente regulamento. A Autoridade Europeia para a Proteção de Dados deve ter competências para impor coimas às instituições, órgãos e organismos da União que se enquadram no âmbito do presente regulamento.

(85) Para assegurar que é possível adaptar o quadro regulamentar quando necessário, o poder de adotar atos nos termos do artigo 290.º do TFUE deverá ser delegado na Comissão no que diz respeito à alteração da legislação de harmonização da União enumerada no anexo II, da lista de sistemas de IA de risco elevado constante do anexo III, das disposições relativas à documentação técnica que constam do anexo IV, do conteúdo da declaração de conformidade UE estabelecido no anexo V, das disposições relativas aos procedimentos de avaliação da conformidade que constam dos anexos VI e VII e das disposições que definem os sistemas de IA de risco elevado aos quais se deve aplicar o procedimento de avaliação da conformidade com base na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor[29]. Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados. As referidas consultas e o apoio consultivo deverão também ser realizados no âmbito das atividades do Comité para a Inteligência Artificial e dos seus subgrupos.

29 JO L 123 de 12.5.2016, p. 1.

(86) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[30]. É particularmente importante que, em conformidade com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor, sempre que sejam necessários conhecimentos especializados mais vastos na preparação inicial dos projetos de atos de execução, a Comissão recorra a grupos de peritos, consulte as partes interessadas específicas ou realize consultas públicas, conforme adequado. As referidas consultas e o apoio consultivo deverão também ser realizados no âmbito das atividades do Comité para a Inteligência Artificial e dos seus subgrupos, incluindo a preparação dos atos de execução relacionados com os artigos 4.º, 4.º-B e 6.º.

(87) Atendendo a que o objetivo do presente regulamento não pode ser suficientemente alcançado pelos Estados-Membros e pode, devido à dimensão ou aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do TUE. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para atingir aquele objetivo.

(87-A) A fim de garantir a segurança jurídica, assegurar um período de adaptação adequado para os operadores e evitar perturbações do mercado, nomeadamente assegurando a continuidade da utilização dos sistemas de IA, é conveniente que o presente regulamento só seja aplicável aos sistemas de IA de risco elevado que tenham sido colocados no mercado ou colocados em serviço antes da data geral de aplicação do mesmo, se, a partir dessa data, esses sistemas estiverem sujeitos a alterações significativas na sua conceção ou finalidade prevista.
É conveniente clarificar que, a este respeito, o conceito de alteração significativa deverá ser entendido como equivalente, em substância, ao conceito de modificação substancial, que é utilizado apenas no que diz respeito aos sistemas de IA de risco elevado, tal como definidos no presente regulamento.

---

30 Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

(88) O presente regulamento deverá aplicar-se a partir de … [*Serviço das Publicações – inserir a data estabelecida no artigo 85.º*]. Contudo, as estruturas relacionadas com a governação e o sistema de avaliação da conformidade deverão estar operacionais antes dessa data, pelo que as disposições relativas aos organismos notificados e à estrutura de governação devem aplicar-se a partir de … [*Serviço das Publicações – inserir a data correspondente a três meses a contar da data de entrada em vigor do presente regulamento*]. Além disso, os Estados-Membros devem estabelecer as regras em matéria de sanções, incluindo coimas, e notificá-las à Comissão, bem como assegurar que sejam aplicadas de forma efetiva e adequada à data de aplicação do presente regulamento. Como tal, as disposições relativas às sanções deverão aplicar-se a partir de … [*Serviço das Publicações – inserir a data correspondente a doze meses a contar da data de entrada em vigor do presente regulamento*].

(89) A Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados foram consultados nos termos do artigo 42.º, n.º 2, do Regulamento (UE) 2018/1725, e emitiram parecer em […],

ADOTARAM O PRESENTE REGULAMENTO:

TÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto

O presente regulamento estabelece:

a) Regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de inteligência artificial ("sistemas de IA") na União;

a) Proibições de certas práticas de inteligência artificial;

b) Requisitos específicos para sistemas de IA de risco elevado e obrigações para os operadores desses sistemas;

c) Regras de transparência harmonizadas para determinados sistemas de IA;

d) Regras relativas à fiscalização do mercado, à vigilância do mercado e à governação;

e) Medidas de apoio à inovação.

Artigo 2.º

Âmbito

1. O presente regulamento é aplicável a:

a) Fornecedores que coloquem no mercado ou coloquem em serviço sistemas de IA no território da União, independentemente de estarem fisicamente presentes ou estabelecidos na União ou num país terceiro;

b) Utilizadores de sistemas de IA que estejam fisicamente presentes ou estabelecidos na União;

c) Fornecedores e utilizadores de sistemas de IA que estejam fisicamente presentes ou estabelecidos num país terceiro, se o resultado produzido pelo sistema for utilizado na União;

d) Importadores e distribuidores de sistemas de IA;

e) Fabricantes de produtos que coloquem no mercado ou coloquem em serviço um sistema de IA juntamente com o seu produto e sob o seu próprio nome ou marca;

f) Mandatários dos prestadores, que estejam estabelecidos na União;

2. Aos sistemas de IA classificados como sistemas de IA de risco elevado em conformidade com o artigo 6.º, n.ºs 1 e 2, relacionados com os produtos abrangidos pela legislação de harmonização da União enumerada no anexo II, secção B, apenas é aplicável o artigo 84.º do presente regulamento. O artigo 53.º só é aplicável na medida em que os requisitos aplicáveis aos sistemas de IA de risco elevado previstos no presente regulamento tenham sido integrados ao abrigo dessa legislação de harmonização da União.

3. O presente regulamento não se aplica aos sistemas de IA se e na medida em que tiverem sido colocados no mercado, colocados em serviço ou utilizados com ou sem modificação desses sistemas para atividades não abrangidas pelo âmbito de aplicação do direito da União e, em qualquer caso, para atividades militares, de defesa ou de segurança nacional, independentemente do tipo de entidade que realiza essas atividades.

   Além disso, o presente regulamento não se aplica aos sistemas de IA que não tenham sido colocados no mercado ou colocados em serviço na União, se os seus resultados forem utilizados na União para atividades não abrangidas pelo âmbito de aplicação do direito da União e, em qualquer caso, para atividades militares, de defesa ou de segurança nacional, independentemente do tipo de entidade que realiza essas atividades.

4. O presente regulamento não se aplica a autoridades públicas de países terceiros, nem a organizações internacionais abrangidas pelo âmbito do presente regulamento nos termos do n.º 1, quando essas autoridades ou organizações usem sistemas de IA no âmbito de acordos internacionais para efeitos de cooperação policial e judiciária com a União ou com um ou vários Estados-Membros.

5. O presente regulamento não afeta a aplicação das disposições relativas à responsabilidade dos prestadores intermediários de serviços estabelecidas no capítulo II, secção 4, da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho[31] [*a substituir pelas disposições correspondentes do Regulamento Serviços Digitais*].

6. O presente regulamento não se aplica a sistemas de IA, incluindo os respetivos resultados, especificamente desenvolvidos e colocados em serviço exclusivamente para fins de investigação e desenvolvimento científicos.

7. O presente regulamento não se aplica às atividades de investigação e desenvolvimento relativas a sistemas de IA.

8. O presente regulamento não se aplica às obrigações dos utilizadores que sejam pessoas singulares que utilizam sistemas de IA no âmbito de uma atividade puramente pessoal de caráter não profissional, com exceção do artigo 52.º.

---

31 Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno ("Diretiva sobre o comércio eletrónico") (JO L 178 de 17.7.2000, p. 1).

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

(1) "Sistema de inteligência artificial" (sistema de IA), um sistema concebido para funcionar com elementos de autonomia e que, com base em dados e entradas fornecidos por máquinas e/ou por seres humanos, que infere a forma de alcançar um determinado conjunto de objetivos utilizando abordagens de aprendizagem automática e/ou abordagens baseadas na lógica e no conhecimento e que produz resultados criados por sistemas, tais como conteúdos (sistemas de IA generativa), previsões, recomendações ou decisões, que influenciam os ambientes com os quais o sistema de IA interage;

1-A) "Ciclo de vida de um sistema de IA", a duração de um sistema de IA, desde a conceção até à reforma. Sem prejuízo dos poderes das autoridades de fiscalização do mercado, essa reforma pode ocorrer em qualquer momento durante a fase de acompanhamento pós-comercialização, mediante decisão do fornecedor, e implica que o sistema não possa continuar a ser utilizado. O ciclo de vida de um sistema de IA também termina se o fornecedor ou qualquer outra pessoa singular ou coletiva efetuar uma modificação substancial do sistema de IA; nesse caso, o sistema de IA substancialmente modificado deve ser considerado um novo sistema de IA.

1-B) "Sistema de IA de finalidade geral", um sistema de IA – independentemente da forma em que tenha sido colocado no mercado ou colocado em serviço, inclusive como software de fonte aberta – cujo fornecedor preveja que desempenha funções de aplicação geral, como o reconhecimento de imagem e de fala, a reprodução de áudio e vídeo, a deteção de padrões, a resposta a perguntas, a tradução, entre outras; um sistema de IA de finalidade geral pode ser utilizado em múltiplos contextos e ser integrado em vários outros sistemas de IA;

(2) "Fornecedor", uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que desenvolva um sistema de IA ou que tenha um sistema de IA desenvolvido e o coloca no mercado ou em serviço sob o seu próprio nome ou marca, a título oneroso ou gratuito;

(3) [suprimido];

3-A) "Pequena e média empresa" (PME), uma empresa tal como definida no anexo da Recomendação 2003/361/CE da Comissão relativa à definição de micro, pequenas e médias empresas;

4) "Utilizador", uma pessoa singular ou coletiva, inclusive uma autoridade pública, agência ou outro organismo, sob cuja autoridade o sistema é utilizado;

5) "Mandatário", uma pessoa singular ou coletiva fisicamente presente ou estabelecida na União que tenha recebido e aceite um mandato escrito de um fornecedor de um sistema de IA para, respetivamente, executar e cumprir em seu nome as obrigações e os procedimentos previstos no presente regulamento;

5-A) "Fabricante de produtos", um fabricante na aceção de qualquer legislação de harmonização da União enumerada no anexo II;

6) "Importador", uma pessoa singular ou coletiva fisicamente presente ou estabelecida na União que coloca no mercado um sistema de IA que ostenta o nome ou a marca de uma pessoa singular ou coletiva estabelecida fora da União;

7) "Distribuidor", uma pessoa singular ou coletiva inserida na cadeia de abastecimento, distinta do fornecedor e do importador, que disponibiliza um sistema de IA no mercado da União;

8) "Operador", um fornecedor, fabricante do produto, utilizador, mandatário, importador ou distribuidor;

9) "Colocação no mercado", a primeira disponibilização de um sistema de IA no mercado da União;

10) "Disponibilização no mercado", o fornecimento de um sistema de IA para distribuição ou utilização no mercado da União no âmbito de uma atividade comercial, a título oneroso ou gratuito;

11) "Colocação em serviço", o fornecimento de um sistema de IA para a primeira utilização na União, diretamente ao utilizador ou para utilização própria, para a finalidade prevista;

12) "Finalidade prevista", a utilização à qual o fornecedor destina o sistema de IA, incluindo o contexto específico e as condições de utilização, conforme especificado nas informações facultadas pelo fornecedor nas instruções de utilização, nos materiais e declarações promocionais ou de venda, bem como na documentação técnica;

13) "Utilização indevida razoavelmente previsível", a utilização de um sistema de IA de uma forma não conforme com a sua finalidade prevista, mas que pode resultar de comportamentos humanos ou de interações com outros sistemas razoavelmente previsíveis;

14) "Componente de segurança de um produto ou sistema", um componente de um produto ou sistema que cumpre uma função de segurança nesse produto ou sistema ou cuja falha ou anomalia põe em risco a segurança e a saúde de pessoas ou bens;

15) "Instruções de utilização", as informações facultadas pelo fornecedor para esclarecer o utilizador, em especial, sobre a finalidade prevista e a utilização correta de um sistema de IA;

16) "Recolha de um sistema de IA", qualquer medida que vise obter a devolução ao fornecedor ou suspender ou desativar a utilização de um sistema de IA disponibilizado aos utilizadores;

17) "Retirada de um sistema de IA", qualquer medida que vise impedir que um sistema de IA presente no circuito comercial seja disponibilizado no mercado;

18) "Desempenho de um sistema de IA", a capacidade de um sistema de IA para alcançar a sua finalidade prevista;

19) "Avaliação da conformidade", o processo de verificar se estão preenchidos os requisitos relacionados com um sistema de IA de risco elevado estabelecidos no título III, capítulo 2, do presente regulamento;

20) "Autoridade notificadora", a autoridade nacional responsável por estabelecer e executar os procedimentos necessários para a avaliação, designação e notificação de organismos de avaliação da conformidade e pela fiscalização destes;

21) "Organismo de avaliação da conformidade", um organismo que realiza atividades de avaliação da conformidade por terceiros, nomeadamente testagem, certificação e inspeção;

22) "Organismo notificado", um organismo de avaliação da conformidade designado nos termos do presente regulamento ou de outra legislação de harmonização da União aplicável;

23) "Modificação substancial", uma alteração do sistema de IA após a sua colocação no mercado ou colocação em serviço que afeta a conformidade do sistema de IA com os requisitos estabelecidos no título III, capítulo 2, do presente regulamento, ou uma modificação da finalidade prevista relativamente à qual o sistema de IA foi avaliado. No respeitante aos sistemas de IA de risco elevado que continuam a aprender após a colocação no mercado ou a colocação em serviço, as alterações introduzidas no sistema de IA de risco elevado e no seu desempenho que tenham sido predeterminadas pelo fornecedor aquando da avaliação da conformidade inicial e façam parte das informações contidas na documentação técnica a que se refere o anexo IV, ponto 2, alínea f), não constituem uma modificação substancial.

24) "Marcação de conformidade CE" (marcação CE), a marcação pela qual um fornecedor atesta que um sistema de IA está em conformidade com os requisitos estabelecidos no título III, capítulo 2, ou no artigo 4.º-B do presente regulamento e nos restantes atos legislativos da União aplicáveis que harmonizam as condições de comercialização de produtos ("legislação de harmonização da União") em que seja prevista a respetiva aposição;

25) "Sistema de acompanhamento pós-comercialização", todas as atividades que os fornecedores de sistemas de IA empreendem para recolher e analisar dados sobre a experiência adquirida com a utilização de sistemas de IA que colocaram no mercado ou em serviço, com vista a identificar a eventual necessidade de aplicar imediatamente quaisquer medidas corretivas ou preventivas necessárias;

26) "Autoridade de fiscalização do mercado", a autoridade nacional que realiza as atividades e toma as medidas previstas no Regulamento (UE) 2019/1020;

27) "Norma harmonizada", uma norma europeia, na aceção do artigo 2.º, n.º 1, alínea c), do Regulamento (UE) n.º 1025/2012;

28) "Especificação comum", um conjunto de especificações técnicas, na aceção do artigo 2.º, ponto 4, do Regulamento (UE) n.º 1025/2012, que oferecem um meio para cumprir certos requisitos estabelecidos no presente regulamento;

29) "Dados de treino", os dados usados para treinar um sistema de IA mediante o ajustamento dos seus parâmetros passíveis de serem aprendidos;

30) "Dados de validação", os dados utilizados para realizar uma avaliação do sistema de IA treinado e para ajustar os seus parâmetros não passíveis de serem aprendidos e o seu processo de aprendizagem, a fim de, entre outros objetivos, evitar um sobreajustamento; sendo que o conjunto de dados de validação pode ser um conjunto de dados separado ou parte de um conjunto de dados de treino, quer como divisão fixa ou variável;

31) "Dados de teste", os dados utilizados para realizar uma avaliação independente do sistema de IA treinado e validado, a fim de confirmar o desempenho esperado desse sistema antes de ser colocado no mercado ou em serviço;

32) "Dados de entrada", os dados fornecidos a um sistema de IA, ou por ele obtidos diretamente, com base nos quais o sistema produz um resultado;

33) "Dados biométricos", dados pessoais resultantes de um tratamento técnico específico das características físicas, fisiológicas ou comportamentais de uma pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

34) "Sistema de reconhecimento de emoções", um sistema de IA concebido para identificar ou inferir estados psicológicos, emoções ou intenções de pessoas singulares com base nos seus dados biométricos;

35) "Sistema de categorização biométrica", um sistema de IA concebido para classificar pessoas singulares em categorias específicas, com base nos seus dados biométricos;

36) "Sistema de identificação biométrica à distância", um sistema de IA concebido para identificar pessoas singulares, normalmente à distância, sem o seu envolvimento ativo, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos num repositório de dados de referência;

37) "Sistema de identificação biométrica à distância "em tempo real"", um sistema de identificação biométrica à distância em que a recolha de dados biométricos, a comparação e a identificação ocorrem de imediato ou quase de imediato;

38) [suprimido]

39) "Espaço acessível ao público", qualquer espaço físico, público ou privado, acessível a um número indeterminado de pessoas singulares, independentemente da predeterminação de certas condições ou circunstâncias de acesso e independentemente das eventuais restrições de capacidade;

40) "Autoridade policial":

a) Uma autoridade pública competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas; ou

b) Qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer autoridade pública e poderes públicos para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas;

41) "Manutenção da ordem pública", as atividades realizadas por autoridades policiais ou em nome destas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas;

42) [suprimido]

43) "Autoridade nacional competente", qualquer das seguintes: a autoridade notificadora ou a autoridade de fiscalização do mercado. No que diz respeito aos sistemas de IA colocados em serviço ou utilizados pelas instituições, agências, serviços e organismos da UE, a Autoridade Europeia para a Proteção de Dados cumpre as responsabilidades que, nos Estados-Membros, são confiadas à autoridade nacional competente e, se for caso disso, qualquer referência às autoridades nacionais competentes ou às autoridades de fiscalização do mercado no presente regulamento deve ser entendida como uma referência à Autoridade Europeia para a Proteção de Dados;

44) "Incidente grave", qualquer incidente ou anomalia num sistema de IA que, direta ou indiretamente, tenha alguma das seguintes consequências:

a) A morte de uma pessoa ou danos graves para a saúde de uma pessoa;

b) Uma perturbação grave e irreversível da gestão e do funcionamento de uma infraestrutura crítica;

c) Uma violação das obrigações decorrentes do direito da União destinadas a proteger os direitos fundamentais;

d) Danos graves a bens ou ao ambiente.

45) "Infraestrutura crítica", um bem, um sistema ou parte dele que seja necessário para a prestação de um serviço essencial para a manutenção de funções societais ou atividades económicas vitais, na aceção do artigo 2.º, pontos 4 e 5, da Diretiva …../….. relativa à resiliência das entidades críticas;

46) "Dados pessoais", os dados na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679;

47) "Dados não pessoais", os dados que não sejam dados pessoais na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679;

48) "Testagem em condições reais", a testagem temporária de um sistema de IA para a sua finalidade prevista em condições reais fora de um laboratório ou de outro ambiente simulado, com vista a recolher dados fiáveis e sólidos e a avaliar e verificar a conformidade do sistema de IA com os requisitos do presente regulamento; a testagem em condições reais não deve ser considerada como colocação no mercado ou colocação em serviço do sistema de IA na aceção do presente regulamento, desde que estejam preenchidas todas as condições previstas no artigo 53.º ou no artigo 54.º-A;

49) "Plano de testagem em condições reais", um documento que descreve os objetivos, a metodologia, o âmbito geográfico, populacional e temporal, o acompanhamento, a organização e a realização dos testes em condições reais;

50) "Participante", para efeitos de testagem em condições reais, uma pessoa singular que participa na testagem em condições reais;

51) "Consentimento informado", a expressão livre e voluntária, por parte do participante, da sua vontade de participar numa dada testagem em condições reais, depois de ter sido informado de todos os aspetos da testagem que sejam relevantes para a sua decisão de participar; no caso de menores e de participantes incapazes, o consentimento informado é dado pelo seu representante legalmente autorizado;

52) "Ambiente de testagem da regulamentação da IA", um quadro concreto criado por uma autoridade nacional competente que oferece aos fornecedores ou potenciais fornecedores de sistemas de IA a possibilidade de desenvolver, treinar, validar e testar, se for caso disso em condições reais, um sistema de IA inovador, de acordo com um plano específico durante um período limitado sob supervisão regulamentar.

Artigo 4.º

Atos de execução

A fim de assegurar condições uniformes para a execução do presente regulamento no que diz respeito às abordagens de aprendizagem automática e às abordagens baseadas na lógica e no conhecimento a que se refere o artigo 3.º, n.º 1, a Comissão pode adotar atos de execução para especificar os elementos técnicos dessas abordagens, tendo em conta a evolução tecnológica e do mercado. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

TÍTULO I-A

SISTEMAS DE IA DE FINALIDADE GERAL

Artigo 4.º-A

Conformidade dos sistemas de IA de finalidade geral com o presente regulamento

1. Sem prejuízo dos artigos 5.º, 52.º, 53.º e 69.º do presente regulamento, os sistemas de IA de finalidade geral cumprem exclusivamente os requisitos e obrigações estabelecidos no artigo 4.º-B.

2. Esses requisitos e obrigações são aplicáveis independentemente de o sistema de IA de finalidade geral ser colocado no mercado ou colocado em serviço como modelo pré-treinado e de o utilizador do sistema de IA de finalidade geral ter de realizar um ajustamento adicional do modelo.

Artigo 4.º-B

Requisitos específicos para sistemas de IA de finalidade geral e obrigações para os fornecedores desses sistemas

1. Os sistemas de IA de finalidade geral que possam ser utilizados como sistemas de IA de risco elevado ou como componentes de sistemas de IA de risco elevado na aceção do artigo 6.º cumprem os requisitos estabelecidos no título III, capítulo 2, do presente regulamento, a partir da data de aplicação dos atos de execução adotados pela Comissão pelo procedimento de exame a que se refere o artigo 74.º, n.º 2, o mais tardar 18 meses após a entrada em vigor do presente regulamento. Esses atos de execução especificam e adaptam a aplicação dos requisitos estabelecidos no título III, capítulo 2, aos sistemas de IA de finalidade geral à luz das suas características, viabilidade técnica, especificidades da cadeia de valor da IA e da evolução tecnológica e do mercado. Ao cumprir esses requisitos, é tido em conta o estado da técnica geralmente reconhecido.

2. Os fornecedores de sistemas de IA de finalidade geral a que se refere o n.º 1 cumprem, a partir da data de aplicação dos atos de execução referidos no n.º 1, as obrigações estabelecidas nos artigos 16.º-AA, 16.º-E, 16.º-F, 16.º-G, 16.º-I, 16.º-J, 25.º, 48.º e 61.º.

3. Para efeitos do cumprimento das obrigações estabelecidas no artigo 16.º-E, os fornecedores seguem o procedimento de avaliação da conformidade baseado no controlo interno previsto no anexo VI, pontos 3 e 4.

4. Os fornecedores desses sistemas também mantêm a documentação técnica a que refere o artigo 11.º à disposição das autoridades nacionais competentes por um período que termina dez anos após a colocação do sistema de IA de finalidade geral no mercado da União ou a sua colocação em serviço na União.

5. Os fornecedores de sistemas de IA de finalidade geral cooperam com outros fornecedores que pretendam colocar em serviço esses sistemas ou colocá-los no mercado da União como sistemas de IA de risco elevado ou componentes de sistemas de IA de risco elevado, e prestam-lhes as informações necessárias, a fim de permitir que estes últimos cumpram as obrigações que lhes incumbem por força do presente regulamento. Essa cooperação entre fornecedores preserva, se for caso disso, os direitos de propriedade intelectual e as informações comerciais confidenciais ou segredos comerciais, em conformidade com o artigo 70.º. A fim de assegurar condições uniformes para a execução do presente regulamento no que diz respeito às informações a partilhar pelos fornecedores de sistemas de IA de finalidade geral, a Comissão pode adotar atos de execução pelo procedimento de exame a que se refere o artigo 74.º, n.º 2.

6. No cumprimento dos requisitos e obrigações a que se referem os n.ºs 1, 2 e 3:

– qualquer referência à finalidade prevista é entendida como referindo-se à possível utilização dos sistemas de IA de finalidade geral como sistemas de IA de risco elevado ou como componentes de sistemas de IA de risco elevado na aceção do artigo 6.º;

– qualquer referência aos requisitos aplicáveis aos sistemas de IA de risco elevado constantes do título III, capítulo II, é entendida como referindo-se apenas aos requisitos estabelecidos no presente artigo.

Artigo 4.º-C

Exceções ao artigo 4.º-B

1. O artigo 4.º-B não é aplicável se o fornecedor tiver excluído explicitamente todas as utilizações de risco elevado nas instruções de utilização ou nas informações que acompanham o sistema de IA de finalidade geral.

2. Essa exclusão é efetuada de boa-fé e não é considerada justificada se o fornecedor tiver razões suficientes para considerar que o sistema pode ser utilizado indevidamente.

3. Sempre que detete ou seja informado de uma utilização indevida no mercado, o fornecedor toma todas as medidas necessárias e proporcionadas para prevenir essa utilização indevida, em especial tendo em conta a escala da utilização indevida e a gravidade dos riscos associados.

TÍTULO II

PRÁTICAS DE INTELIGÊNCIA ARTIFICIAL PROIBIDAS

Artigo 5.º

1. Estão proibidas as seguintes práticas de inteligência artificial:

a) A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que empregue técnicas subliminares que contornem a consciência de uma pessoa com o objetivo ou efeito de distorcer substancialmente o seu comportamento de uma forma que cause ou seja razoavelmente suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

b) A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que explore quaisquer vulnerabilidades de um grupo específico de pessoas associadas à sua idade, deficiência ou situação socioeconómica específica, com o objetivo ou efeito de distorcer substancialmente o comportamento de uma pessoa pertencente a esse grupo de uma forma que cause ou seja razoavelmente suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

c) A colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA para efeitos de avaliação ou classificação de pessoas singulares durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais, conhecidas ou previsíveis, em que a classificação social conduz a uma das seguintes situações ou a ambas:

i) tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos das mesmas em contextos sociais não relacionados com os contextos nos quais os dados foram originalmente gerados ou recolhidos;

ii) tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos das mesmas que é injustificado ou desproporcionado face ao seu comportamento social ou à gravidade do mesmo;

d) A utilização de sistemas de identificação biométrica à distância em "tempo real" em espaços acessíveis ao público por autoridades policiais ou em nome destas para efeitos de manutenção da ordem pública, salvo se essa utilização for estritamente necessária para alcançar um dos seguintes objetivos:

i) a investigação seletiva de potenciais vítimas específicas de crimes,

ii) a prevenção de uma ameaça específica e substancial à infraestrutura crítica, à vida, à saúde ou à segurança física de pessoas singulares ou a prevenção de ataques terroristas,

iii) a localização ou identificação de uma pessoa singular para efeitos da realização de uma investigação criminal, instauração de ação penal ou execução de uma sanção penal por infrações referidas no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho[32] e puníveis no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos, ou outras infrações específicas puníveis no Estado-Membro em causa por uma pena ou medida de segurança privativas de liberdade de duração máxima não inferior a cinco anos, e tal como definidas pela legislação desse Estado-Membro.

2. A utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve ter em conta os seguintes elementos:

a) A natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos prejuízos causados na ausência da utilização do sistema;

---

32 Decisão-quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO L 190 de 18.7.2002, p. 1).

b) As consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências.

Além disso, a utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve observar salvaguardas e condições necessárias e proporcionadas em relação a tal utilização, nomeadamente no respeitante a limitações temporais, geográficas e das pessoas visadas.

3. No tocante ao n.º 1, alínea d), e ao n.º 2, cada utilização de um sistema de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública está sujeita a autorização prévia concedida por uma autoridade judiciária ou por uma autoridade administrativa independente do Estado-Membro no qual a utilização terá lugar após apresentação de um pedido fundamentado em conformidade com as regras de execução previstas no direito nacional a que se refere o n.º 4. Contudo, numa situação de urgência devidamente justificada, a utilização do sistema pode ser iniciada sem uma autorização, desde que essa autorização seja solicitada sem demora injustificada durante a utilização do sistema de IA e, se essa autorização for rejeitada, a sua utilização seja suspensa com efeitos imediatos.

A autoridade judiciária ou administrativa competente apenas deve conceder a autorização se considerar, com base em dados objetivos ou indícios claros que lhe tenham sido apresentados, que a utilização do sistema de identificação biométrica à distância "em tempo real" em apreço é necessária e proporcionada para alcançar um dos objetivos especificados no n.º 1, alínea d), conforme identificado no pedido. Ao decidir sobre o pedido, a autoridade judiciária ou administrativa competente tem em conta os elementos referidos no n.º 2.

4. Um Estado-Membro pode decidir prever a possibilidade de autorizar total ou parcialmente a utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública dentro dos limites e sob as condições enumeradas no n.º 1, alínea d), e nos n.ºs 2 e 3. Esse Estado-Membro estabelece na sua legislação nacional as regras pormenorizadas aplicáveis ao pedido, à emissão e ao exercício das autorizações a que se refere o n.º 3, bem como à supervisão e comunicação das mesmas. Essas regras especificam igualmente em relação a que objetivos enumerados no n.º 1, alínea d), incluindo quais das infrações penais referidas na subalínea iii) da mesma, as autoridades competentes podem ser autorizadas a usar esses sistemas para efeitos de manutenção da ordem pública.

TÍTULO III

SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO

CAPÍTULO 1

CLASSIFICAÇÃO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL COMO SENDO DE RISCO ELEVADO

Artigo 6.º

Regras para a classificação de sistemas de inteligência artificial de risco elevado

1. Um sistema de IA que seja, ele próprio, um produto abrangido pela legislação de harmonização da União enumerada no anexo II deve ser considerado de risco elevado se tiver de ser sujeito a uma avaliação da conformidade por terceiros com vista à sua colocação no mercado ou entrada em serviço nos termos da referida legislação.

2. Um sistema de IA destinado a ser utilizado como componente de segurança de um produto abrangido pela legislação a que se refere o n.º 1 deve ser considerado de risco elevado se tiver de ser sujeito a uma avaliação da conformidade por terceiros com vista à sua colocação no mercado ou entrada em serviço nos termos da referida legislação. Esta disposição é aplicável independentemente de o sistema de IA ser colocado no mercado ou colocado em serviço separadamente do produto.

3. Os sistemas de IA referidos no anexo III são considerados de risco elevado, a menos que os resultados do sistema sejam puramente acessórios no que diz respeito às ações ou decisões pertinentes a tomar e, por conseguinte, não sejam suscetíveis de conduzir a um risco significativo para a saúde, a segurança ou os direitos fundamentais.

A fim de assegurar condições uniformes para a execução do presente regulamento, a Comissão adota, o mais tardar um ano após a entrada em vigor do presente regulamento, atos de execução para especificar as circunstâncias em que os resultados dos sistemas de IA referidos no anexo III seriam puramente acessórios no que diz respeito às ações ou decisões pertinentes a tomar. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 7.º

Alterações do anexo III

1. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para alterar a lista do anexo III, aditando sistemas de IA de risco elevado que preencham ambas as condições que se seguem:

a) Os sistemas de IA destinam-se a ser utilizados em qualquer um dos domínios enumerados no anexo III, pontos 1 a 8;

b) Os sistemas de IA representam um risco de danos para a saúde e a segurança ou um risco de impacto adverso nos direitos fundamentais que, em termos de gravidade e probabilidade de ocorrência, é equivalente ou superior ao risco de danos ou impacto adverso representado pelos sistemas de IA de risco elevado já referidos no anexo III.

2. Ao avaliar, para efeitos do disposto no n.º 1, se um sistema de IA representa um risco de danos para a saúde e a segurança ou um risco de impacto adverso nos direitos fundamentais equivalente ou superior ao risco de danos representado pelos sistemas de IA de risco elevado já referidos no anexo III, a Comissão tem em consideração os seguintes critérios:

a) A finalidade prevista do sistema de IA;

b) O grau de utilização efetiva ou a probabilidade de utilização de um sistema de IA;

c) Em que medida a utilização de um sistema de IA já causou danos para a saúde e a segurança ou um impacto adverso nos direitos fundamentais ou suscitou preocupações significativas quanto à concretização desses danos ou desse impacto adverso, conforme demonstrado por relatórios ou alegações documentadas apresentadas às autoridades nacionais competentes;

d) O potencial grau desses danos ou desse impacto adverso, nomeadamente em termos de intensidade e de capacidade para afetar um grande número de pessoas;

e) O grau de dependência das pessoas potencialmente lesadas ou adversamente afetadas em relação ao resultado produzido por um sistema de IA, em especial se, por razões práticas ou jurídicas, aquelas não puderem razoavelmente autoexcluir-se desse resultado;

f) A posição de vulnerabilidade das pessoas potencialmente prejudicadas ou adversamente afetadas em relação ao utilizador de um sistema de IA, nomeadamente devido a um desequilíbrio de poder ou de conhecimento, a circunstâncias económicas ou sociais, ou à idade;

g) A dificuldade de reversão do resultado produzido com um sistema de IA, tendo em conta que os resultados com impacto na saúde ou na segurança das pessoas não podem ser considerados como facilmente reversíveis;

h) Em que medida a legislação da União em vigor prevê:

i) medidas de reparação eficazes em relação aos riscos representados por um sistema de IA, com exclusão de pedidos de indemnização,

ii) medidas eficazes para prevenir ou minimizar substancialmente esses riscos;

i) a magnitude e a probabilidade de benefício da utilização da IA para os indivíduos, os grupos ou a sociedade em geral.

3. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para alterar a lista do anexo III, suprimindo sistemas de IA de risco elevado que preencham ambas as condições que se seguem:

a) O(s) sistema(s) de IA de risco elevado em causa deixam de representar qualquer risco significativo para os direitos fundamentais, a saúde ou a segurança, tendo em conta os critérios enumerados no n.º 2;

b) A supressão não diminui o nível geral de proteção da saúde, da segurança e dos direitos fundamentais ao abrigo do direito da União.

CAPÍTULO 2

REQUISITOS APLICÁVEIS A SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO

Artigo 8.º

Cumprimento dos requisitos

1. Os sistemas de IA de risco elevado devem cumprir os requisitos estabelecidos no presente capítulo, tendo em conta o estado da técnica geralmente reconhecido.

2. A finalidade prevista do sistema de IA de risco elevado e o sistema de gestão de riscos a que se refere o artigo 9.º devem ser tidos em conta para efeitos do cumprimento desses requisitos.

Artigo 9.º

Sistema de gestão de riscos

1. Deve ser criado, implantado, documentado e mantido um sistema de gestão de riscos em relação a sistemas de IA de risco elevado.

2. O sistema de gestão de riscos é entendido como um processo iterativo contínuo, planeado e executado ao longo de todo o ciclo de vida de um sistema de IA de risco elevado, o que requer atualizações regulares sistemáticas. Deve compreender as seguintes etapas:

   a) Identificação e análise dos riscos conhecidos e previsíveis mais suscetíveis de ocorrer para a saúde, a segurança e os direitos fundamentais, tendo em conta a finalidade prevista do sistema de IA de risco elevado;

   b) [suprimido];

   c) Avaliação de outros riscos que possam surgir, baseada na análise dos dados recolhidos a partir do sistema de acompanhamento pós-comercialização a que se refere o artigo 61.º;

   d) Adoção de medidas de gestão de riscos adequadas em conformidade com o disposto nos números que se seguem.

   O presente número faz referência apenas aos riscos que possam ser razoavelmente atenuados ou eliminados durante o desenvolvimento ou a conceção do sistema de IA de risco elevado ou da prestação de informações técnicas adequadas.

3. As medidas de gestão de riscos a que se refere o n.º 2, alínea d), devem ter em devida consideração os efeitos e eventual interação resultantes da aplicação combinada dos requisitos estabelecidos no presente capítulo, com vista a minimizar os riscos de forma mais eficaz e, ao mesmo tempo, alcançar um equilíbrio adequado na aplicação das medidas destinadas a cumprir esses requisitos.

4. As medidas de gestão de riscos a que se refere o n.º 2, alínea d), devem levar a que o eventual risco residual associado a cada perigo, bem como o risco residual global dos sistemas de IA de risco elevado, sejam considerados aceitáveis.

Ao identificar as medidas de gestão de riscos mais apropriadas, deve assegurar-se o seguinte:

a) Eliminação ou redução dos riscos identificados e avaliados nos termos do n.º 2, tanto quanto possível através da conceção e do desenvolvimento adequados do sistema de IA de risco elevado;

b) Se for caso disso, adoção de medidas de atenuação e controlo adequadas em relação a riscos que não possam ser eliminados;

c) Prestação de informações adequadas nos termos do artigo 13.º, em especial no atinente aos riscos a que se refere o n.º 2, alínea b), do presente artigo e, se for caso disso, formação dos utilizadores.

Com vista à eliminação ou redução de riscos relacionados com a utilização do sistema de IA de risco elevado, há que ter em consideração o conhecimento técnico, a experiência, a educação e a formação que se pode esperar que o utilizador possua e o ambiente em que está previsto utilizar o sistema.

5. Os sistemas de IA de risco elevado são sujeitos a testes a fim de assegurar que os sistemas de IA de risco elevado funcionem de forma coerente com a finalidade prevista e que cumpram os requisitos estabelecidos no presente capítulo.

6. Os procedimentos de teste podem incluir a testagem em condições reais, em conformidade com o artigo 54.º-A.

7. Os testes dos sistemas de IA de risco elevado devem ser realizados, consoante apropriado, em qualquer momento durante o processo de desenvolvimento e, em qualquer caso, antes da colocação no mercado ou da colocação em serviço. Os testes devem ser realizados relativamente a métricas previamente definidas e a limiares probabilísticos que são apropriados para a finalidade prevista do sistema de IA de risco elevado.

8. O sistema de gestão de riscos descrito nos n.ºs 1 a 7, toma especificamente em conta se o sistema de IA de risco elevado é suscetível de ser acedido por pessoas com menos de 18 anos ou de ter impacto nas mesmas.

9. Para os fornecedores de sistemas de IA de risco elevado sujeitos a requisitos relativos aos processos internos de gestão de riscos nos termos do direito setorial aplicável da União, os aspetos descritos nos n.ºs 1 a 8 podem fazer parte dos procedimentos de gestão de riscos estabelecidos nos termos desse direito.

Artigo 10.º

Dados e governação de dados

1. Os sistemas de IA de risco elevado que utilizem técnicas que envolvam o treino de modelos com dados devem ser desenvolvidos com base em conjuntos de dados de treino, validação e teste que cumpram os critérios de qualidade referidos nos n.ºs 2 a 5.

2. Os conjuntos de dados de treino, validação e teste devem estar sujeitos a práticas adequadas de governação e gestão de dados. Essas práticas dizem nomeadamente respeito:

   a) Às escolhas de conceção tomadas;

   b) A processos de recolha de dados;

   c) Às operações de preparação e tratamento de dados necessárias, tais como anotação, rotulagem, limpeza, enriquecimento e agregação;

d) À formulação dos pressupostos aplicáveis, nomeadamente no que diz respeito às informações que os dados devem medir e representar;

e) À avaliação prévia da disponibilidade, quantidade e adequação dos conjuntos de dados que são necessários;

f) Ao exame para detetar eventuais enviesamentos suscetíveis de afetar a saúde e a segurança das pessoas singulares ou de resultar em discriminações proibidas pelo direito da União;

g) À identificação de eventuais lacunas ou deficiências de dados e de possíveis soluções para as mesmas.

3. Os conjuntos de dados de treino, validação e teste devem ser pertinentes, representativos e, tanto quanto possível, isentos de erros e completos. Devem ter as propriedades estatísticas adequadas, nomeadamente, quando aplicável, no tocante às pessoas ou grupos de pessoas em que o sistema de IA de risco elevado se destina a ser utilizado. Estas características dos conjuntos de dados podem ser satisfeitas a nível de conjuntos de dados individuais ou de uma combinação dos mesmos.

4. Os conjuntos de dados de treino, validação e teste devem ter em conta, na medida do necessário para a finalidade prevista, as características ou os elementos que são idiossincráticos do enquadramento geográfico, comportamental ou funcional específico no qual o sistema de IA de risco elevado se destina a ser utilizado.

5. Na medida do estritamente necessário para assegurar o controlo, a deteção e a correção de enviesamentos em relação a sistemas de IA de risco elevado, os fornecedores desses sistemas podem tratar categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, o artigo 10.º da Diretiva (UE) 2016/680 e o artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725, assegurando salvaguardas adequadas dos direitos fundamentais e liberdades das pessoas singulares, incluindo impor limitações técnicas à reutilização e utilizar medidas de segurança e preservação da privacidade de última geração, tais como a pseudonimização ou a cifragem nos casos em que a anonimização possa afetar significativamente a finalidade preconizada.

6. Para o desenvolvimento de sistemas de IA de risco elevado que não utilizam técnicas que envolvem o treino de modelos, os n.ºs 2 a 5 aplicam-se apenas aos conjuntos de dados de treino.

Artigo 11.º

Documentação técnica

1. A documentação técnica de um sistema de IA de risco elevado deve ser elaborada antes da colocação no mercado ou colocação em serviço desse sistema e mantida atualizada.

   A documentação técnica deve ser elaborada de maneira que demonstre que o sistema de IA de risco elevado cumpre os requisitos estabelecidos no presente capítulo e deve facultar às autoridades nacionais competentes e aos organismos notificados, de forma clara e completa, todas as informações necessárias para aferir a conformidade do sistema de IA com esses requisitos. A documentação técnica deve conter, no mínimo, os elementos previstos no anexo IV ou, no caso das PME, inclusive empresas em fase de arranque, qualquer documentação equivalente que cumpra os mesmos objetivos, salvo se a autoridade competente o considerar inadequado.

2. Caso um sistema de IA de risco elevado relacionado com um produto, ao qual sejam aplicáveis os atos jurídicos enumerados no anexo II, secção A, seja colocado no mercado ou colocado em serviço, deve ser elaborada uma única documentação técnica que contenha todas as informações enumeradas no anexo IV e as informações exigidas nos termos desses atos jurídicos.

3. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para alterar o anexo IV, se for caso disso, com vista a assegurar que, tendo em conta a evolução técnica, a documentação técnica forneça todas as informações necessárias para aferir a conformidade do sistema com os requisitos estabelecidos no presente capítulo.

Artigo 12.º

Manutenção de registos

1. Os sistemas de IA de risco elevado devem permitir tecnicamente o registo automático de eventos ("registos") ao longo do ciclo de vida do sistema.

2. A fim de assegurar um nível de rastreabilidade do funcionamento do sistema de IA adequado à finalidade prevista do sistema, as capacidades de registo devem permitir o registo de eventos pertinentes para

   i) a identificação de situações que possam dar azo a que o sistema de IA apresente um risco na aceção do artigo 65.º, n.º 1, ou dar origem a uma modificação substancial;

   ii) a facilitação do acompanhamento pós-comercialização a que se refere o artigo 61.º; e

   iii) o controlo do funcionamento dos sistemas de IA de risco elevado a que se refere o artigo 29.º, n.º 4.

4. Em relação aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 1, alínea a), as capacidades de registo devem proporcionar, no mínimo:

   a) O registo do período de cada utilização do sistema (data e hora de início e data e hora de fim de cada utilização);

   b) A base de dados de referência relativamente à qual os dados de entrada foram verificados pelo sistema;

   c) Os dados de entrada cuja pesquisa conduziu a uma correspondência;

   d) A identificação das pessoas singulares envolvidas na verificação dos resultados, conforme referido no artigo 14.º, n.º 5.

Artigo 13.º

Transparência e prestação de informações aos utilizadores

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que assegure que o seu funcionamento seja suficientemente transparente, com vista a garantir o cumprimento das obrigações que incumbem ao utilizador e ao fornecedor por força do capítulo 3 do presente título e a permitir que os utilizadores compreendam e utilizem o sistema de forma adequada.

2. Os sistemas de IA de risco elevado devem ser acompanhados de instruções de utilização, num formato digital ou outro adequado, que incluam informações concisas, completas, corretas e claras que sejam pertinentes, acessíveis e compreensíveis para os utilizadores.

3. As informações a que se refere o n.º 2 devem especificar:

   a) A identidade e os dados de contacto do fornecedor e, se for caso disso, do seu mandatário;

   b) As características, capacidades e limitações de desempenho do sistema de IA de risco elevado, incluindo:

      i) a finalidade prevista do sistema, incluindo o enquadramento geográfico, comportamental ou funcional específico no qual o sistema de IA de risco elevado se destina a ser utilizado;

      ii) o nível de exatidão, nomeadamente a sua métrica, de solidez e de cibersegurança a que se refere o artigo 15.º relativamente ao qual o sistema de IA de risco elevado foi testado e validado e que pode ser esperado, bem como quaisquer circunstâncias conhecidas e previsíveis que possam ter um impacto nesse nível esperado de exatidão, solidez e cibersegurança,

      iii) qualquer circunstância conhecida ou previsível, relacionada com a utilização do sistema de IA de risco elevado de acordo com a sua finalidade prevista, que possa causar os riscos a que se refere o artigo 9.º, n.º 2, para a saúde e a segurança ou para os direitos fundamentais,

iv) quando oportuno, o seu comportamento em relação a determinadas pessoas ou grupos de pessoas em que o sistema se destina a ser utilizado,

v) quando oportuno, especificações para os dados de entrada, ou quaisquer outras informações importantes em termos dos conjuntos de dados de treino, validação e teste usados, tendo em conta a finalidade prevista do sistema de IA;

vi) quando oportuno, a descrição dos resultados esperados do sistema.

c) As alterações do sistema de IA de risco elevado e do seu desempenho que foram predeterminadas pelo fornecedor aquando da avaliação da conformidade inicial, se for caso disso;

d) As medidas de supervisão humana a que se refere o artigo 14.º, incluindo as soluções técnicas adotadas para facilitar a interpretação dos resultados dos sistemas de IA pelos utilizadores;

e) Os recursos computacionais e de hardware necessários, a vida útil esperada do sistema de IA de risco elevado e quaisquer medidas de manutenção e assistência necessárias, incluindo a sua frequência, para assegurar o correto funcionamento desse sistema de IA, inclusive no tocante a atualizações do software;

f) Uma descrição do mecanismo incluído no sistema de IA que permita aos utilizadores recolher, armazenar e interpretar corretamente os registos, se for caso disso.

Artigo 14.º

Supervisão humana

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de tal modo, incluindo com ferramentas de interface homem-máquina apropriadas, que possam ser eficazmente supervisionados por pessoas singulares durante o período de utilização do sistema de IA.

2. A supervisão humana deve procurar prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de IA de risco elevado é usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, em especial quando esses riscos persistem apesar da aplicação de outros requisitos estabelecidos neste capítulo.

3. A supervisão humana deve ser assegurada por meio de um ou de todos os seguintes tipos de medidas:

   a) Medidas identificadas e integradas, quando tecnicamente viável, pelo fornecedor no sistema de IA de risco elevado antes de este ser colocado no mercado ou colocado em serviço;

   b) Medidas identificadas pelo fornecedor antes de o sistema de IA de risco elevado ser colocado no mercado ou colocado em serviço e que sejam adequadas para implantação por parte do utilizador.

4. Para efeitos da aplicação dos n.ºs 1 a 3, o sistema de IA de risco elevado deve ser fornecido ao utilizador de forma a que as pessoas singulares responsáveis pela supervisão humana, em função das circunstâncias e proporcionalmente às mesmas:

   a) Compreendam as capacidades e limitações do sistema de IA de risco elevado e sejam capazes de controlar devidamente o seu funcionamento;

   b) Estejam conscientes da possível tendência para confiar automaticamente ou confiar excessivamente no resultado produzido pelo sistema de IA de risco elevado ("enviesamento da automatização"):

   c) Interpretem corretamente o resultado do sistema de IA de risco elevado, tendo em conta, por exemplo, as ferramentas e os métodos de interpretação disponíveis;

   d) Decidam, em qualquer situação específica, não usar o sistema de IA de risco elevado ou ignorar, anular ou reverter os resultados do sistema de IA de risco elevado;

   e) Intervenham no funcionamento do sistema de IA de risco elevado ou interrompam o sistema por meio de um botão de "paragem" ou procedimento similar.

5. Em relação aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 1, alínea a), as medidas referidas no n.º 3 devem, além disso, permitir assegurar que nenhuma ação ou decisão seja tomada pelo utilizador com base na identificação resultante do sistema, salvo se a mesma tiver sido verificada e confirmada separadamente por, pelo menos, duas pessoas singulares. O requisito de verificação separada por, pelo menos, duas pessoas singulares não se aplica aos sistemas de IA de risco elevado utilizados para efeitos de manutenção da ordem pública, de migração, de controlo das fronteiras ou de asilo, nos casos em que o direito da União ou nacional considere que a aplicação deste requisito é desproporcionada.

Artigo 15.º

Exatidão, solidez e cibersegurança

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que alcancem, tendo em conta a finalidade prevista, um nível apropriado de exatidão, solidez e cibersegurança e apresentem um desempenho coerente em relação a tais aspetos durante o ciclo de vida.

2. As instruções de utilização que acompanham os sistemas de IA de risco elevado devem declarar os níveis de exatidão e a métrica de exatidão aplicável.

3. Os sistemas de IA de risco elevado devem ser resistentes a erros, falhas ou incoerências que possam ocorrer no sistema ou no ambiente em que aquele opera, em especial devido à interação com pessoas singulares ou outros sistemas.

A solidez dos sistemas de IA de risco elevado pode ser alcançada por via de soluções de redundância técnica, que podem incluir planos de reserva ou de segurança à prova de falhas.

Os sistemas de IA de risco elevado que continuam a aprender após a colocação no mercado ou a colocação em serviço são desenvolvidos de forma a eliminar ou reduzir, tanto quanto possível, o risco de resultados possivelmente enviesados que influenciem futuras operações ("circuitos de realimentação"), bem como a assegurar que esses resultados possivelmente enviesados são devidamente abordados por via de medidas de atenuação adequadas.

4. Os sistemas de IA de risco elevado devem ser resistentes a tentativas de terceiros não autorizados de alterar a sua utilização ou desempenho explorando as vulnerabilidades do sistema.

As soluções técnicas destinadas a assegurar a cibersegurança dos sistemas de IA de risco elevado devem ser adequadas às circunstâncias e aos riscos de cada caso.

As soluções técnicas para resolver vulnerabilidades específicas da inteligência artificial devem incluir, se for caso disso, medidas para prevenir e controlar ataques que visem manipular o conjunto de dados de treino ("contaminação de dados"), dados de entrada preparados para fazer com que o modelo cometa um erro ("exemplos antagónicos"), ou falhas do modelo.

CAPÍTULO 3

OBRIGAÇÕES DOS FORNECEDORES E UTILIZADORES DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO E DE OUTRAS PARTES

Artigo 16.º

Obrigações dos fornecedores de sistemas de inteligência artificial de risco elevado

Os fornecedores de sistemas de IA de risco elevado devem:

(a) Assegurar que os seus sistemas de IA de risco elevado cumprem os requisitos estabelecidos no capítulo 2 do presente título;

a-A) Indicar o seu nome, nome comercial registado ou marca registada, endereço de contacto no sistema de IA de risco elevado, ou, se tal não for possível, na respetiva embalagem ou na documentação que o acompanha, conforme aplicável;

b) Dispor de um sistema de gestão da qualidade que cumpra o disposto no artigo 17.º;

c) Conservar a documentação, nos termos do artigo 18.º;

d) Quando tal esteja sob o seu controlo, manter os registos gerados automaticamente pelos sistemas de IA de risco elevado que fornecem, tal como referido no artigo 20.º;

e) Assegurar que o sistema de IA de risco elevado seja sujeito ao procedimento de avaliação da conformidade aplicável, tal como referido no artigo 43.º, antes da colocação no mercado ou da colocação em serviço;

f) Respeitar as obrigações de registo a que se refere o artigo 51.º, n.º1;

g) Adotar as medidas corretivas necessárias mencionadas no artigo 21.º, se o sistema de IA de risco elevado não estiver em conformidade com os requisitos estabelecidos no capítulo 2 do presente título;

h) Informar a autoridade nacional competente dos Estados-Membros nos quais disponibilizaram o sistema de IA ou o colocaram em serviço e, se for caso disso, o organismo notificado sobre a não conformidade e quaisquer medidas corretivas tomadas;

i) Apor a marcação CE nos sistemas de IA de risco elevado para indicar a conformidade com o presente regulamento de acordo com o artigo 49.º;

j) Mediante pedido de uma autoridade nacional competente, demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título.

Artigo 17.º

Sistema de gestão da qualidade

1. Os fornecedores de sistemas de IA de risco elevado devem criar um sistema de gestão da qualidade que assegure a conformidade com o presente regulamento. Esse sistema deve estar documentado de uma forma sistemática e ordenada, sob a forma de políticas, procedimentos e instruções escritas, e deve incluir, no mínimo, os seguintes aspetos:

   a) Uma estratégia para o cumprimento da regulamentação, incluindo a observância de procedimentos de avaliação da conformidade e de procedimentos de gestão de modificações do sistema de IA de risco elevado;

b) Técnicas, procedimentos e ações sistemáticas a utilizar para a conceção, controlo da conceção e verificação da conceção do sistema de IA de risco elevado;

c) Técnicas, procedimentos e ações sistemáticas a utilizar para o desenvolvimento, controlo da qualidade e garantia da qualidade do sistema de IA de risco elevado;

d) Procedimentos de exame, teste e validação a realizar antes, durante e após o desenvolvimento do sistema de IA de risco elevado e a frequência com a qual têm de ser realizados;

e) Especificações técnicas, incluindo normas, a aplicar e, se as normas harmonizadas em causa não forem aplicadas na íntegra, os meios a usar para assegurar que o sistema de IA de risco elevado cumpra os requisitos estabelecidos no capítulo 2 do presente título;

f) Sistemas e procedimentos de gestão de dados, incluindo recolha de dados, análise de dados, rotulagem de dados, armazenamento de dados, filtragem de dados, prospeção de dados, agregação de dados, conservação de dados e qualquer outra operação relativa aos dados que seja realizada antes e para efeitos da colocação no mercado ou colocação em serviço de sistemas de IA de risco elevado;

g) O sistema de gestão de riscos a que se refere o artigo 9.º;

h) O estabelecimento, aplicação e manutenção de um sistema de acompanhamento pós-comercialização, nos termos do artigo 61.º;

i) Procedimentos de comunicação de um incidente grave em conformidade com o artigo 62.º;

j) A gestão da comunicação com autoridades nacionais competentes, autoridades competentes, incluindo as setoriais, disponibilizando ou apoiando o acesso a dados, organismos notificados, outros operadores, clientes ou outras partes interessadas;

k) Sistemas e procedimentos de manutenção de registos de toda a documentação e informação importante;

l) Gestão de recursos, incluindo medidas relacionadas com a segurança do aprovisionamento;

m) Um quadro que defina as responsabilidades do pessoal com funções de gestão e do restante pessoal no atinente a todos os aspetos elencados no presente número.

2. A aplicação dos aspetos referidos no n.º 1 deve ser proporcionada à dimensão da organização do fornecedor.

2-A. Para os fornecedores de sistemas de IA de risco elevado sujeitos a obrigações relativas aos sistemas de gestão da qualidade nos termos do direito setorial aplicável da União, os aspetos descritos no n.º 1 podem fazer parte dos sistemas de gestão da qualidade estabelecidos nos termos desse direito.

3. Para os fornecedores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos ao abrigo da legislação da União no domínio dos serviços financeiros, considera-se que a obrigação de criar um sistema de gestão da qualidade, com exceção do n.º 1, alíneas g), h) e i), é satisfeita mediante o cumprimento das regras relativas a sistemas ou processos de governação interna nos termos da legislação da União aplicável em matéria de serviços financeiros. Neste contexto, devem ser tidas em conta quaisquer normas harmonizadas referidas no artigo 40.º do presente regulamento.

Artigo 18.º

Manutenção de documentação

1. O fornecedor deve manter à disposição das autoridades nacionais competentes, durante os dez anos subsequentes à data de colocação no mercado ou de colocação em serviço do sistema de IA:

a) A documentação técnica a que se refere o artigo 11.º;

b) A documentação relativa ao sistema de gestão da qualidade a que se refere o artigo 17.º;

c) A documentação relativa às alterações aprovadas pelos organismos notificados, se for caso disso;

d) As decisões e outros documentos emitidos pelos organismos notificados, se for caso disso;

e) A declaração de conformidade UE a que se refere o artigo 48.º.

1-A. Cada Estado-Membro determina as condições em que a documentação a que se refere o n.º 1 permanece à disposição das autoridades nacionais competentes durante o período indicado nesse número, nos casos em que um fornecedor ou o seu mandatário estabelecido no seu território falir ou cessar a sua atividade antes do termo desse período.

2. Os fornecedores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos ao abrigo da legislação da União no domínio dos serviços financeiros devem manter a documentação técnica como parte da documentação conservada ao abrigo da legislação da União aplicável em matéria de serviços financeiros.

Artigo 19.º

Avaliação da conformidade

1. Os fornecedores de sistemas de IA de risco elevado devem assegurar que os sistemas que fornecem são sujeitos a um procedimento de avaliação da conformidade de acordo com o artigo 43.º, antes de serem colocados no mercado ou colocados em serviço. Assim que a conformidade dos sistemas de IA com os requisitos estabelecidos no capítulo 2 do presente título tiver sido demonstrada na sequência de uma avaliação da conformidade, os fornecedores devem elaborar uma declaração de conformidade UE de acordo com o artigo 48.º e apor a marcação de conformidade CE de acordo com o artigo 49.º.

2. [suprimido]

Artigo 20.º

Registos gerados automaticamente

1. Os fornecedores de sistemas de IA de risco elevado devem manter os registos a que se refere o artigo 12.º, n.º 1, gerados automaticamente pelos respetivos sistemas de IA de risco elevado, desde que esses registos estejam sob o seu controlo por força de uma disposição contratual com o utilizador ou de uma disposição legal. Devem conservá-los por um período mínimo de seis meses, salvo disposição em contrário na legislação da União ou nacional aplicável, em especial no direito da União em matéria de proteção de dados pessoais.

2. Os fornecedores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos ao abrigo da legislação da União no domínio dos serviços financeiros devem manter os registos gerados automaticamente pelos sistemas de IA de risco elevado que fornecem como parte da documentação conservada ao abrigo da legislação aplicável em matéria de serviços financeiros.

Artigo 21.º

Medidas corretivas

Os fornecedores de sistemas de IA de risco elevado que considerem ou tenham motivos para crer que um sistema de IA de risco elevado que colocaram no mercado ou colocaram em serviço não está em conformidade com o presente regulamento devem imediatamente investigar, se for caso disso, as causas, em colaboração com o utilizador comunicador, e tomar as medidas corretivas necessárias para repor a conformidade do sistema em questão ou proceder à retirada ou recolha do mesmo, consoante o caso. Devem igualmente informar do facto os distribuidores do sistema de IA de risco elevado em questão e, se for caso disso, o mandatário e os importadores.

Artigo 22.º

Dever de informação

Se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, e esse risco for do conhecimento do fornecedor do sistema, este último deve informar imediatamente as autoridades nacionais competentes dos Estados-Membros nos quais disponibilizou o sistema e, se for caso disso, o organismo notificado que emitiu um certificado para o sistema de IA de risco elevado, em especial sobre a não conformidade e quaisquer as medidas corretivas tomadas.

Artigo 23.º

Cooperação com as autoridades competentes

Os fornecedores de sistemas de IA de risco elevado devem, mediante pedido de uma autoridade nacional competente, prestar a essa autoridade todas as informações e documentação necessárias para demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, numa língua que possa ser facilmente compreendida pela autoridade do Estado-Membro em questão. Mediante pedido fundamentado de uma autoridade nacional competente, os fornecedores devem igualmente conceder a essa autoridade o acesso aos registos, a que se refere o artigo 12.º, n.º 1, gerados automaticamente pelo sistema de IA de risco elevado, desde que esses registos estejam sob o seu controlo por força de uma disposição contratual com o utilizador ou de uma disposição legal.

Artigo 23.º-A

Condições para sujeitar outras pessoas às obrigações de um fornecedor

1. Qualquer pessoa singular ou coletiva é considerada um fornecedor de um sistema de IA de alto risco para efeitos do presente regulamento e é sujeita às obrigações do fornecedor estabelecidas no artigo 16.º em qualquer uma das seguintes circunstâncias:

    a) Se colocar o seu nome ou marca num sistema de IA de risco elevado já colocado no mercado ou colocado em serviço, sem prejuízo de disposições contratuais que estipulem uma atribuição diferente das obrigações;

b) [suprimido]

c) Se modificar substancialmente um sistema de IA de risco elevado já colocado no mercado ou colocado em serviço;

d) Se modificar a finalidade prevista de um sistema de IA que não é de risco elevado e que já tenha sido colocado no mercado ou colocado em serviço, de tal forma que o transforme num sistema de IA de risco elevado;

e) Se colocar no mercado ou colocar em serviço um sistema de IA de finalidade geral como sistema de IA de risco elevado ou como componente de um sistema de IA de risco elevado.

2. Sempre que se verificarem as circunstâncias a que se refere o n.º 1, alíneas a) ou c), o fornecedor que inicialmente colocou no mercado ou colocou em serviço o sistema de IA de risco elevado deixa de ser considerado um fornecedor para efeitos do presente regulamento.

3. No caso dos sistemas de IA de risco elevado que sejam componentes de segurança de produtos aos quais se apliquem os atos jurídicos enunciados no anexo II, secção A, o fabricante desses produtos deve ser considerado o fornecedor do sistema de IA de risco elevado e deve ficar sujeito às obrigações estabelecidas no artigo 16.º, em qualquer um dos seguintes cenários:

i) o sistema de IA de risco elevado é colocado no mercado juntamente com o produto sob o nome ou marca do respetivo fabricante,

ii) o sistema de IA de risco elevado é colocado em serviço sob o nome ou marca do fabricante do produto, depois de o produto ter sido colocado no mercado.

Artigo 24.º

[suprimido]

Artigo 25.º

Mandatários

1. Antes de disponibilizarem os seus sistemas no mercado da União, os fornecedores estabelecidos fora da União devem, através de mandato escrito, designar um mandatário estabelecido na União.

2. O mandatário deve praticar os atos definidos no mandato conferido pelo fornecedor. Para efeitos do presente regulamento, o mandato habilita o mandatário a exercer apenas as seguintes funções:

-a) Verificar se a declaração de conformidade UE e a documentação técnica foram elaboradas e se o fornecedor efetuou um procedimento de avaliação da conformidade adequado;

a) Manter à disposição das autoridades nacionais competentes e das autoridades nacionais a que se refere o artigo 63.º, n.º 7, durante um período de 10 anos a contar da data de colocação no mercado ou colocação em serviço do sistema de IA de risco elevado, os dados de contacto do fornecedor pelo qual o mandatário foi designado, uma cópia da declaração de conformidade UE, a documentação técnica e, se aplicável, o certificado emitido pelo organismo notificado;

b) Prestar a uma autoridade nacional competente, mediante pedido fundamentado, todas as informações e documentação necessárias, inclusive as conservadas em conformidade com a alínea b), para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, incluindo o acesso aos registos, a que se refere o artigo 12.º, n.º 1, gerados automaticamente pelo sistema de IA de risco elevado, desde que esses registos se encontrem sob o controlo do fornecedor por força de uma disposição contratual com o utilizador ou de uma disposição legal;

c) Cooperar com as autoridades nacionais competentes, mediante pedido fundamentado, em qualquer ação que estas empreendam em relação ao sistema de IA de risco elevado.

d) Cumprir as obrigações de registo a que se refere o artigo 51.º, n.º 1, e, se o registo do sistema for efetuado pelo próprio fornecedor, verificar se as informações a que se refere o anexo VIII, parte II, pontos 1 a 11, estão corretas.

O mandatário põe termo ao mandato se tiver razões suficientes para considerar que o fornecedor não cumpre as obrigações que lhe incumbem por força do presente regulamento. Nesse caso, informa de imediato a autoridade de fiscalização do mercado do Estado-Membro no qual está estabelecido, bem como, se for caso disso, o organismo notificado pertinente, da cessação do mandato e da respetiva justificação.

O mandatário é legalmente responsável por sistemas de IA defeituosos nas mesmas condições e solidariamente com o fornecedor no que respeita à sua potencial responsabilidade nos termos da Diretiva 85/374/CEE do Conselho.

Artigo 26.º

Obrigações dos importadores

1. Antes de colocarem um sistema de IA de risco elevado no mercado, os importadores desse sistema devem assegurar-se de que esse sistema está em conformidade com o presente regulamento verificando se:

a) O fornecedor desse sistema de IA realizou o procedimento de avaliação da conformidade em causa a que se refere o artigo 43.º;

b) O fornecedor elaborou a documentação técnica em conformidade com o anexo IV;

c) O sistema ostenta a marcação de conformidade CE exigida e está acompanhado da declaração de conformidade UE e das instruções de utilização;

d) O fornecedor designou o mandatário a que se refere o artigo 25.º.

2. Se um importador tiver motivos suficientes para crer que um sistema de IA de risco elevado não está em conformidade com o presente regulamento, ou é falsificado ou acompanhado de documentação falsificada, não coloca esse sistema de IA no mercado enquanto o mesmo não for tornado conforme. Se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, o importador deve informar desse facto o fornecedor do sistema de IA, os mandatários e as autoridades de fiscalização do mercado.

3. Os importadores devem indicar o seu nome, nome comercial registado ou marca registada e endereço de contacto no sistema de IA de risco elevado, ou, se tal não for possível, na respetiva embalagem ou na documentação que o acompanha, conforme aplicável.

4. Enquanto um sistema de IA de risco elevado estiver sob a responsabilidade dos importadores, estes devem assegurar, se for caso disso, que as condições de armazenamento ou de transporte não prejudicam a conformidade do sistema com os requisitos enunciados no capítulo 2 do presente título.

4-A. Os importadores devem conservar, por um período de 10 anos a contar da data de colocação no mercado ou colocação em serviço do sistema de IA, uma cópia do certificado emitido pelo organismo notificado, quando aplicável, das instruções de utilização e da declaração de conformidade UE.

5. Os importadores devem prestar às autoridades nacionais competentes, mediante pedido fundamentado, todas as informações e documentação necessárias, inclusive as conservadas em conformidade com o n.º 5, para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, numa língua que possa ser facilmente compreendida pela autoridade nacional competente em causa. Para o efeito, assegura igualmente que a documentação técnica possa ser disponibilizada a essas autoridades.

5-A. Os importadores devem cooperar com as autoridades nacionais competentes em qualquer ação que estas empreendam em relação a um sistema de IA de que sejam importadores.

Artigo 27.º

Obrigações dos distribuidores

1. Antes de disponibilizarem um sistema de IA de risco elevado no mercado, os distribuidores verificam se o sistema de IA de risco elevado ostenta a marcação de conformidade CE exigida, se está acompanhado de uma cópia da declaração de conformidade UE e das instruções de utilização necessárias e se o fornecedor e o importador do sistema, consoante o caso, cumpriram as obrigações estabelecidas no artigo 16.º, alínea b), e no artigo 26.º, n.º 3, respetivamente.

2. Se um distribuidor considerar ou tiver motivos para crer que um sistema de IA de risco elevado não está em conformidade com os requisitos estabelecidos no capítulo 2 do presente título, não pode disponibilizar esse sistema de IA de risco elevado no mercado enquanto o mesmo não for tornado conforme com os referidos requisitos. Além disso, se o sistema apresentar um risco na aceção do artigo 65.º, n.º 1, o distribuidor deve informar desse facto o fornecedor ou o importador do sistema, conforme o caso.

3. Enquanto um sistema de IA de risco elevado estiver sob a responsabilidade dos distribuidores, estes devem assegurar, se for caso disso, que as condições de armazenamento ou de transporte não prejudicam a conformidade do sistema com os requisitos enunciados no capítulo 2 do presente título.

4. Um distribuidor que considere ou tenha motivos para crer que um sistema de IA de risco elevado que disponibilizou no mercado não em conformidade com os requisitos estabelecidos no capítulo 2 do presente título deve tomar as medidas corretivas necessárias para repor a conformidade desse sistema com os referidos requisitos, proceder à retirada ou recolha do mesmo ou assegurar que o fornecedor, o importador ou qualquer operador envolvido, consoante o caso, toma essas medidas corretivas. Se um sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, o distribuidor deve informar imediatamente desse facto as autoridades nacionais competentes dos Estados-Membros em que disponibilizou o produto, apresentando dados, sobretudo no que se refere à não conformidade e às medidas corretivas tomadas.

5. Mediante pedido fundamentado de uma autoridade nacional competente, os distribuidores de sistemas de IA de risco elevado prestam a essa autoridade todas as informações e documentação relativas às suas atividades, conforme descrito nos n.ºs 1 a 4.

5-A. Os distribuidores cooperam com as autoridades nacionais competentes em qualquer ação que essas autoridades tomem em relação a um sistema de IA de que sejam distribuidores.

Artigo 28.º

[suprimido]

Artigo 29.º

Obrigações dos utilizadores de sistemas de inteligência artificial de risco elevado

1. Os utilizadores de sistemas de IA de risco elevado devem utilizá-los de acordo com as instruções de utilização que acompanham os sistemas, nos termos dos n.ºs 2 e 5 do presente artigo.

1-A. Os utilizadores atribuem a supervisão humana a pessoas singulares que possuam as competências, a formação e a autoridade necessárias.

2. As obrigações previstas nos n.ºs 1 e 1-A não excluem outras obrigações do utilizador previstas na legislação da União ou nacional nem prejudicam o poder discricionário do utilizador para organizar os seus próprios recursos e atividades para efeitos de aplicação das medidas de supervisão humana indicadas pelo fornecedor.

3. Sem prejuízo do disposto no n.º 1, desde que o utilizador exerça controlo sobre os dados de entrada, esse utilizador deve assegurar que os dados de entrada sejam adequados à finalidade prevista do sistema de IA de risco elevado.

4. Os utilizadores aplicam a supervisão humana e controlam o funcionamento do sistema de IA de risco elevado com base nas instruções de utilização. Se tiverem motivos para considerar que a utilização de acordo com as instruções de utilização pode fazer com que o sistema de IA apresente um risco na aceção do artigo 65.º, n.º 1, devem informar o fornecedor ou distribuidor e suspender a utilização do sistema. Devem também informar o fornecedor ou distribuidor e interromper a utilização do sistema de IA caso identifiquem qualquer incidente grave. Se o utilizador não conseguir entrar em contacto com o fornecedor, aplica-se, por analogia, o artigo 62.º. Esta obrigação não abrange os dados operacionais sensíveis dos utilizadores de sistemas de IA que sejam autoridades policiais.

Em relação aos fornecedores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos ao abrigo da legislação da União no domínio dos serviços financeiros, considera-se que a obrigação de controlo estabelecida no primeiro parágrafo é satisfeita mediante o cumprimento das regras relativas a sistemas, processos e mecanismos de governação interna previstas na legislação aplicável em matéria de serviços financeiros.

5. Os utilizadores de sistemas de IA de risco elevado devem manter os registos, a que se refere o artigo 12.º, n.º 1, gerados automaticamente por esse sistema de IA de risco elevado, desde que esses registos estejam sob o seu controlo. Devem conservá-los por um período mínimo de seis meses, salvo disposição em contrário na legislação da União ou nacional aplicável, em especial no direito da União em matéria de proteção de dados pessoais.

Os utilizadores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos ao abrigo da legislação da União no domínio dos serviços financeiros devem manter os registos como parte da documentação conservada nos termos da legislação da União aplicável em matéria de serviços financeiros.

5-A. Os utilizadores de sistemas de IA de risco elevado que sejam autoridades, agências ou organismos públicos, com exceção das autoridades policiais, de controlo das fronteiras, de imigração ou de asilo, devem cumprir as obrigações de registo a que se refere o artigo 51.º. Se verificarem que o sistema que tencionam utilizar não foi registado na base de dados da UE a que se refere o artigo 60.º, não devem utilizar esse sistema e devem informar o fornecedor ou o distribuidor.

6. Os utilizadores de sistemas de IA de risco elevado devem usar as informações recebidas nos termos do artigo 13.º para cumprirem a sua obrigação de realizar uma avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º do Regulamento (UE) 2016/679 ou do artigo 27.º da Diretiva (UE) 2016/680, conforme aplicável.

6-A. Os utilizadores devem cooperar com as autoridades nacionais competentes em qualquer ação que essas autoridades tomem em relação a um sistema de IA de que são utilizadores.

CAPÍTULO 4

AUTORIDADES NOTIFICADORAS E ORGANISMOS NOTIFICADOS

Artigo 30.º

Autoridades notificadoras

1. Cada Estado-Membro deve designar ou criar pelo menos uma autoridade notificadora responsável por estabelecer e executar os procedimentos necessários para a avaliação, a designação e a notificação de organismos de avaliação da conformidade e pela fiscalização destes.

2. Os Estados-Membros podem decidir que a avaliação e o controlo referidos no n.º 1 sejam efetuados por um organismo nacional de acreditação, na aceção e nos termos do Regulamento (CE) n.º 765/2008.

3. As autoridades notificadoras devem ser criadas, organizadas e geridas de maneira que garanta a ausência de conflitos de interesses com os organismos de avaliação da conformidade e a objetividade e imparcialidade das suas atividades.

4. As autoridades notificadoras devem estar organizadas de maneira que as decisões relativas à notificação dos organismos de avaliação da conformidade sejam tomadas por pessoas competentes diferentes daquelas que realizaram a avaliação desses organismos.

5. As autoridades notificadoras não podem propor nem desempenhar qualquer atividade que seja da competência dos organismos de avaliação da conformidade, nem prestar quaisquer serviços de consultoria com caráter comercial ou em regime de concorrência.

6. As autoridades notificadoras devem proteger a confidencialidade das informações obtidas em conformidade com o artigo 70.º.

7. As autoridades notificadoras devem dispor de recursos humanos com competência técnica em número adequado para o correto exercício das suas funções.

8. [suprimido]

Artigo 31.º

Apresentação de pedido de notificação por um organismo de avaliação da conformidade

1. Os organismos de avaliação da conformidade devem apresentar um pedido de notificação à autoridade notificadora do Estado-Membro onde se encontram estabelecidos.

2. O pedido de notificação deve ser acompanhado de uma descrição das atividades de avaliação da conformidade, do módulo ou dos módulos de avaliação da conformidade e dos sistemas de IA em relação aos quais o organismo se considera competente, bem como de um certificado de acreditação, se existir, emitido por um organismo nacional de acreditação, que ateste que o organismo de avaliação da conformidade cumpre os requisitos estabelecidos no artigo 33.º Deve ser igualmente anexado qualquer documento válido relacionado com designações vigentes do organismo notificado requerente ao abrigo de qualquer outra legislação de harmonização da União.

3. Se não lhe for possível apresentar o certificado de acreditação, o organismo de avaliação da conformidade deve fornecer à autoridade notificadora todas as provas documentais necessárias à verificação, ao reconhecimento e à fiscalização regular da sua conformidade com os requisitos estabelecidos no artigo 33.º. Em relação aos organismos notificados designados ao abrigo de qualquer outra legislação de harmonização da União, todos os documentos e certificados associados a essas designações podem ser usados para fundamentar o seu processo de designação nos termos do presente regulamento, consoante adequado. O organismo notificado atualiza a documentação referida nos n.ºs 2 e 3 sempre que ocorram alterações relevantes, a fim de permitir que a autoridade nacional responsável pelos organismos notificados monitorize e verifique o cumprimento permanente de todos os requisitos estabelecidos no artigo 33.º.

Artigo 32.º

Procedimento de notificação

1. As autoridades notificadoras apenas podem notificar os organismos de avaliação da conformidade que cumpram os requisitos previstos no artigo 33.º

2. As autoridades notificadoras devem notificar a Comissão e os restantes Estados-Membros sobre esses organismos utilizando um instrumento de notificação eletrónica criado e gerido pela Comissão.

3. A notificação a que se refere o n.º 2 deve incluir dados pormenorizados das atividades de avaliação da conformidade, do módulo ou módulos de avaliação da conformidade e dos sistemas de IA em causa, bem como a certificação de competência relevante. Caso a notificação não se baseie no certificado de acreditação referido no artigo 31.º, n.º 2, a autoridade notificadora deve fornecer à Comissão e aos outros Estados-Membros provas documentais que atestem a competência técnica do organismo de avaliação da conformidade e as disposições introduzidas para assegurar que o organismo seja auditado periodicamente e continue a cumprir os requisitos previstos no artigo 33.º.

4. O organismo de avaliação da conformidade em causa apenas pode efetuar as atividades reservadas a organismos notificados se nem a Comissão nem os outros Estados-Membros tiverem formulado objeções nas duas semanas seguintes a uma notificação por uma autoridade notificadora, se esta incluir um certificado de acreditação a que se refere o artigo 31.º, n.º 2, ou nos dois meses seguintes a uma notificação por uma autoridade notificadora, se esta incluir as provas documentais a que se refere o artigo 31.º, n.º 3.

5. [suprimido]

Artigo 33.º

Requisitos aplicáveis aos organismos notificados

1. Os organismos notificados devem ser constituídos nos termos da lei nacional e ser dotados de personalidade jurídica.

2. Os organismos notificados devem satisfazer os requisitos em termos de organização, gestão da qualidade, recursos e processos que sejam necessários para o exercício das suas tarefas.

3. A estrutura organizacional, a atribuição de responsabilidades, a cadeia hierárquica e o funcionamento dos organismos notificados devem ser de molde a assegurar a confiança no desempenho e nos resultados das atividades de avaliação da conformidade que os organismos notificados realizam.

4. Os organismos notificados devem ser independentes do fornecedor de um sistema de IA de risco elevado relativamente ao qual realizam atividades de avaliação da conformidade. Os organismos notificados devem também ser independentes de qualquer outro operador que tenha um interesse económico no sistema de IA de risco elevado que é avaliado, bem como de quaisquer concorrentes do fornecedor.

5. Os organismos notificados devem estar organizados e funcionar de maneira que garanta a independência, a objetividade e a imparcialidade das suas atividades. Os organismos notificados devem documentar e estabelecer uma estrutura e procedimentos capazes de salvaguardar essa imparcialidade e de promover e aplicar os princípios da imparcialidade em toda a sua organização, pessoal e atividades de avaliação.

6. Os organismos notificados devem dispor de procedimentos documentados que garantam que o seu pessoal, comités, filiais, subcontratantes e qualquer outro organismo associado ou pessoal de organismos externos respeitam a confidencialidade das informações em conformidade com o artigo 70.º de que tenham conhecimento durante a realização das atividades de avaliação da conformidade, salvo se a divulgação daquelas for exigida por lei. O pessoal dos organismos notificados deve estar sujeito ao sigilo profissional no que se refere a todas as informações que obtiver no exercício das suas funções no âmbito do presente regulamento, exceto em relação às autoridades notificadoras do Estado-Membro em que exerce as suas atividades.

7. Os organismos notificados devem dispor de procedimentos relativos ao exercício de atividades que tenham em devida conta a dimensão de uma empresa, o setor em que opera, a sua estrutura e o grau de complexidade do sistema de IA em questão.

8. Os organismos notificados devem subscrever um seguro de responsabilidade civil adequado para as suas atividades de avaliação da conformidade, a menos que essa responsabilidade seja assumida pelo Estado-Membro onde se encontram nos termos da legislação nacional ou que esse Estado-Membro seja diretamente responsável pela avaliação da conformidade.

9. Os organismos notificados devem ser capazes de executar todas as tarefas que lhes forem atribuídas pelo presente regulamento com a maior integridade profissional e a competência exigida no domínio específico, quer essas tarefas sejam executadas por eles próprios, quer em seu nome e sob a sua responsabilidade.

10. Os organismos notificados devem dispor de competências internas suficientes para poderem avaliar eficazmente as tarefas realizadas em seu nome por partes externas. Os organismos notificados devem dispor permanentemente de suficiente pessoal administrativo, técnico, jurídico e científico com experiência e conhecimentos relativos às tecnologias de inteligência artificial em apreço, aos dados e à computação de dados e aos requisitos estabelecidos no capítulo 2 do presente título.

11. Os organismos notificados devem participar em atividades de coordenação conforme referido no artigo 38.º. Além disso, devem participar, diretamente ou por meio de representantes, em organizações europeias de normalização, ou assegurar que têm conhecimentos e se mantêm atualizados acerca das normas aplicáveis.

12. [suprimido]

Artigo 33.º-A

Presunção da conformidade com os requisitos aplicáveis aos organismos notificados

Presume-se que os organismos de avaliação da conformidade que provem a sua conformidade com os critérios estabelecidos nas normas harmonizadas aplicáveis, ou em partes destas, cujas referências tenham sido publicadas no Jornal Oficial da União Europeia cumprem os requisitos previstos no artigo 33.º, contanto que as referidas normas harmonizadas contemplem esses requisitos.

Artigo 34.º

Filiais e subcontratantes dos organismos notificados

1. Sempre que um organismo notificado subcontratar tarefas específicas relacionadas com a avaliação da conformidade ou recorrer a uma filial, deve assegurar que o subcontratante ou a filial cumprem os requisitos previstos no artigo 33.º e informar a autoridade notificadora desse facto.

2. Os organismos notificados devem assumir plena responsabilidade pelas tarefas executadas por subcontratantes ou filiais, independentemente do local em que estes se encontram estabelecidos.

3. As atividades só podem ser exercidas por um subcontratante ou por uma filial mediante acordo do fornecedor.

4. Os documentos necessários respeitantes à avaliação das qualificações do subcontratante ou da filial e ao trabalho efetuado por estes nos termos do presente regulamento devem ser mantidos à disposição da autoridade notificadora durante um período de 5 anos a contar da data de termo da atividade de subcontratação.

Artigo 34.º-A

Obrigações operacionais dos organismos notificados

1. Os organismos notificados devem verificar a conformidade de um sistema de IA de risco elevado de acordo com os procedimentos de avaliação da conformidade a que se refere o artigo 43.º.

2. Os organismos notificados devem exercer as suas atividades evitando encargos desnecessários para os fornecedores e tendo em devida conta a dimensão de uma empresa, o setor em que opera, a sua estrutura e o grau de complexidade do sistema de IA de risco elevado em questão. Ao atenderem a estes fatores, os organismos notificados devem, contudo, respeitar o grau de rigor e o nível de proteção exigidos para que o sistemas de IA de risco elevado cumpra os requisitos do presente regulamento.

3. Os organismos notificados devem disponibilizar e, mediante pedido, apresentar toda a documentação importante, incluindo a documentação elaborada pelos fornecedores, à autoridade notificadora a que se refere o artigo 30.º para que essa autoridade possa exercer as suas atividades de avaliação, designação, notificação e controlo e ainda para facilitar a avaliação descrita no presente capítulo.

Artigo 35.º

Números de identificação e listas de organismos notificados designados nos termos do presente regulamento

1. A Comissão atribui um número de identificação aos organismos notificados. O número atribuído é único, mesmo que o organismo esteja notificado ao abrigo de vários atos da União.

2. A Comissão publica a lista de organismos notificados ao abrigo do presente regulamento, incluindo os números de identificação que lhes foram atribuídos e as atividades em relação às quais foram notificados. A Comissão assegura a atualização dessa lista.

Artigo 36.º

Alterações das notificações

1. A autoridade notificadora deve notificar a Comissão e os outros Estados-Membros de quaisquer alterações pertinentes à notificação de um organismo notificado através do instrumento de notificação eletrónica a que se refere o artigo 32.º, n.º 2.

2. Os procedimentos descritos nos artigos 31.º e 32.º aplicam-se ao alargamento do âmbito da notificação. No que respeita às alterações à notificação, à exceção do alargamento do seu âmbito de aplicação, são aplicáveis os procedimentos estabelecidos nos números seguintes.

Caso um organismo notificado decida cessar as suas atividades de avaliação da conformidade, informa a autoridade notificadora e os fornecedores em causa o mais rapidamente possível e, em caso de cessação planeada, um ano antes de cessar as atividades. Os certificados podem manter-se válidos durante um período temporário de nove meses após a cessação das atividades do organismo notificado, desde que outro organismo notificado confirme por escrito que assumirá a responsabilidade pelos sistemas de IA abrangidos por esses certificados. O novo organismo notificado efetua uma avaliação completa dos sistemas de IA em causa até ao final desse período, antes de emitir novos certificados para esses sistemas. Se o organismo notificado tiver cessado a sua atividade, a autoridade notificadora deve retirar a designação.

3. Caso a autoridade notificadora tenha motivos suficientes para considerar que um organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 33.º, ou que não cumpre as suas obrigações, a autoridade notificadora deve restringir, suspender ou retirar a notificação, consoante o caso, em função da gravidade do incumprimento desses requisitos ou dessas obrigações, desde que o organismo notificado tenha tido a possibilidade de expressar as suas observações. Deve informar imediatamente a Comissão e os restantes Estados-Membros deste facto.

4. Caso a sua designação tenha sido suspensa, restringida ou revogada, na totalidade ou em parte, o organismo notificado informa os fabricantes em causa o mais tardar no prazo de 10 dias.

5. Em caso de restrição, suspensão ou retirada de uma notificação, a autoridade notificadora deve tomar as medidas necessárias para assegurar que os processos do organismo notificado são conservados e deve disponibilizá-los às autoridades notificadoras noutros Estados-Membros e às autoridades de fiscalização do mercado, se estas o solicitarem.

6. Em caso de restrição, suspensão ou retirada de uma designação, a autoridade notificadora:

   a) Avalia o impacto nos certificados emitidos pelo organismo notificado;

   b) Apresenta à Comissão e aos outros Estados-Membros um relatório sobre as suas conclusões no prazo de três meses após ter notificado as alterações à notificação;

   c) Determina que o organismo notificado suspenda ou retire, num prazo razoável por ela determinado, os certificados indevidamente emitidos, a fim de garantir a conformidade dos sistemas de IA no mercado;

   d) Informa a Comissão e os Estados-Membros dos certificados cuja suspensão ou retirada tenha exigido;

e) Fornece às autoridades nacionais competentes do Estado-Membro em que o fornecedor tem a sua sede social todas as informações pertinentes sobre os certificados para os quais exigiu a suspensão ou retirada. Essa autoridade competente toma as medidas adequadas que se revelem necessárias para evitar potenciais riscos para a saúde, a segurança ou os direitos fundamentais.

7. Com exceção dos certificados indevidamente emitidos, e caso uma notificação tenha sido suspensa ou restringida, os certificados permanecem válidos nas seguintes circunstâncias:

a) Quando a autoridade notificadora tiver confirmado, no prazo de um mês a contar da suspensão ou restrição, que, no que respeita aos certificados afetados pela suspensão ou restrição, não existem riscos para a saúde, a segurança ou os direitos fundamentais, e tiver estabelecido um prazo e as ações previstas para obviar à suspensão ou restrição; ou

b) Quando a autoridade notificadora tiver confirmado que, durante o período de suspensão ou restrição, não serão emitidos, alterados nem reemitidos certificados relevantes para a suspensão, e declarado se o organismo notificado tem capacidade para continuar a assumir, durante o período da suspensão ou restrição, o controlo e a responsabilidade pelos certificados já emitidos. Caso a autoridade responsável pelos organismos notificados determine que o organismo notificado não tem capacidade para apoiar certificados existentes emitidos, o fornecedor deve fornecer às autoridades nacionais competentes do Estado-Membro em que o fornecedor do sistema abrangido pelo certificado tem a sua sede social, no prazo de três meses a contar da suspensão ou restrição, uma confirmação escrita de que outro organismo notificado qualificado assume temporariamente as funções do organismo notificado de controlar e permanecer responsável pelos certificados durante o período de suspensão ou restrição.

8. Com exceção dos certificados emitidos indevidamente, e sempre que a designação tenha sido retirada, os certificados permanecem válidos por um período de nove meses nas seguintes circunstâncias:

a) Se a autoridade nacional competente do Estado-Membro em que o fornecedor do sistema de IA abrangido pelo certificado tem a sua sede social tiver confirmado que não existem riscos para a saúde, a segurança e os direitos fundamentais associados aos sistemas em questão; e

b) Se um outro organismo notificado tiver confirmado por escrito que assumirá de imediato a responsabilidade por esses sistemas e que concluirá a respetiva avaliação no prazo de doze meses a contar da retirada da designação.

Nas circunstâncias referidas no primeiro parágrafo, a autoridade nacional competente do Estado-Membro em que o fornecedor do sistema abrangido pelo certificado tem a sua sede social pode prorrogar a validade provisória dos certificados por novos períodos de três meses, até um máximo de 12 meses no total.

A autoridade nacional competente ou o organismo notificado que assumir as funções do organismo notificado ao qual se aplica a alteração da notificação informa imediatamente desse facto a Comissão, os outros Estados-Membros e os demais organismos notificados.

Artigo 37.º

Contestação da competência dos organismos notificados

1. A Comissão investiga, sempre que necessário, todos os casos em que haja motivos para duvidar do cumprimento dos requisitos estabelecidos no artigo 33.º por parte de um organismo notificado.

2. A autoridade notificadora deve facultar à Comissão, mediante pedido, todas as informações importantes relacionadas com a notificação do organismo notificado em causa.

3. A Comissão garante que todas as informações confidenciais obtidas no decurso das suas investigações nos termos do presente artigo são tratadas de forma confidencial em conformidade com o artigo 70.º.

4. Caso verifique que um organismo notificado não cumpre ou deixou de cumprir os requisitos estabelecidos no artigo 33.º, a Comissão informa a autoridade notificadora dos motivos dessa verificação e solicita-lhe que tome as medidas corretivas necessárias, incluindo, se for caso disso, a suspensão, a restrição ou a retirada da designação. Se a autoridade notificadora não tomar as medidas corretivas necessárias, a Comissão pode, por meio de atos de execução, suspender, restringir ou retirar a notificação. O referido ato de execução é adotado de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 38.º

Coordenação dos organismos notificados

1. A Comissão assegura que, no respeitante aos sistemas de IA de risco elevado, são instituídas modalidades de coordenação e cooperação adequadas entre organismos notificados ativos nos procedimentos de avaliação da conformidade nos termos do presente regulamento e que as mesmas decorrem devidamente sob a forma de um grupo setorial de organismos notificados.

2. A autoridade notificadora deve assegurar que os organismos por si notificados participam, diretamente ou por meio de representantes designados, nos trabalhos desse grupo.

Artigo 39.º

Organismos de avaliação da conformidade de países terceiros

Os organismos de avaliação da conformidade criados ao abrigo da legislação de um país terceiro com o qual a União tenha celebrado um acordo podem ser autorizados a executar as atividades de organismos notificados nos termos do presente regulamento, desde que cumpram os requisitos do artigo 33.º.

CAPÍTULO 5

NORMAS, AVALIAÇÃO DA CONFORMIDADE, CERTIFICADOS, REGISTO

Artigo 40.º

Normas harmonizadas

1. Presume-se que os sistemas de IA de risco elevado ou os sistemas de IA de finalidade geral que estão em conformidade com normas harmonizadas, ou com partes destas, cujas referências tenham sido publicadas no Jornal Oficial da União Europeia, são conformes com os requisitos estabelecidos no capítulo 2 do presente título, ou, consoante o caso, com os requisitos estabelecidos nos artigos 4.º-A e 4.º-B, desde que tais normas abranjam esses requisitos.

2. Ao enviar um pedido de normalização a uma organização europeia de normalização em conformidade com o artigo 10.º do Regulamento n.º 1025/2012, a Comissão deve especificar que as normas são coerentes, claras e elaboradas de uma forma que permita cumprir, concretamente, os seguintes objetivos:

   a) Garantir que os sistemas de IA colocados no mercado ou colocados em serviço na União sejam seguros e respeitem os valores e reforcem a autonomia estratégica aberta da União;

   b) Promover o investimento e a inovação em IA, nomeadamente através do aumento da segurança jurídica, bem como a competitividade e o crescimento do mercado da União;

   c) Melhorar a governação multilateral, representativa de todas as partes interessadas europeias (por exemplo, indústria, PME, sociedade civil, investigadores);

   d) Contribuir para o reforço da cooperação mundial em matéria de normalização no domínio da IA, compatível com os valores e os interesses da União.

   A Comissão deve solicitar às organizações europeias de normalização que apresentem provas dos seus melhores esforços para cumprir os objetivos acima referidos.

Artigo 41.º

Especificações comuns

1. A Comissão fica habilitada a adotar, após consulta do Comité para a Inteligência Artificial a que se refere o artigo 56.º, atos de execução de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2, que estabeleçam especificações técnicas comuns para os requisitos estabelecidos no capítulo 2 do presente título, ou, se for caso disso, com os requisitos estabelecidos no artigo 4.º-A e no artigo 4.º-B, se estiverem preenchidas as seguintes condições:

   a) Não se encontra publicada no Jornal Oficial da União Europeia qualquer referência a normas harmonizadas que abranjam as preocupações essenciais em termos de segurança ou direitos fundamentais pertinentes, em conformidade com o Regulamento (UE) n.º 1025/2012;

   b) A Comissão pediu, nos termos do artigo 10.º, n.º 1, do Regulamento (CE) n.º 1025/2012, a uma ou mais organizações europeias de normalização que elaborassem uma norma harmonizada para os requisitos estabelecidos no capítulo 2 do presente título;

   c) O pedido a que se refere a alínea b) não foi aceite por nenhuma das organizações europeias de normalização, ou as normas harmonizadas relativas a esse pedido não foram entregues no prazo fixado em conformidade com o artigo 10.º, n.º 1, do Regulamento (CE) n.º 1025/2012, ou essas normas não cumprem o pedido.

1-A. Antes de elaborar um projeto de ato de execução, a Comissão informa o comité a que se refere o artigo 22.º do Regulamento (UE) n.º 1025/2012 de que considera que estão preenchidas as condições previstas no n.º 1.

2. Na preparação inicial do projeto de ato de execução que estabelece as especificações comuns, a Comissão cumpre os objetivos referidos no artigo 40.º, n.º 2, e recolhe os pontos de vista dos organismos ou grupos de peritos pertinentes criados ao abrigo do direito setorial aplicável da União. Com base nessa consulta, a Comissão elabora o projeto de ato de execução.

3. Presume-se que os sistemas de IA de risco elevado ou os sistemas de IA de finalidade geral que estão em conformidade com as especificações comuns a que se refere o n.º 1 são conformes com os requisitos estabelecidos no capítulo 2 do presente título, ou, consoante o caso, com os requisitos estabelecidos nos artigos 4.º-A e 4.º-B, desde que tais especificações comuns abranjam esses requisitos.

4. Quando as referências de uma norma harmonizada forem publicadas no Jornal Oficial da União Europeia, os atos de execução a que se refere o n.º 1, que abranjam os requisitos estabelecidos no capítulo 2 do presente título ou os requisitos estabelecidos nos artigos 4.º-A e 4.º-B, são revogados, conforme aplicável.

5. Se um Estado-Membro considerar que uma especificação comum não satisfaz inteiramente os requisitos estabelecidos no capítulo 2 do presente título ou os requisitos estabelecidos nos artigos 4.º-A e 4.º-B, conforme aplicável, informa a Comissão desse facto, prestando uma explicação pormenorizada, e a Comissão avalia essas informações e, se for caso disso, altera o ato de execução que estabelece a especificação comum em causa.

Artigo 42.º

Presunção de conformidade com determinados requisitos

1. Presume-se que os sistemas de IA de risco elevado que foram treinados e testados com recurso a dados que refletem o enquadramento geográfico, comportamental e funcional específico no qual se destinam a ser utilizados são conformes com os respetivos requisitos estabelecidos no artigo 10.º, n.º 4.

2. Presume-se que os sistemas de IA de risco elevado e os sistemas de IA para finalidade geral que foram certificados ou relativamente aos quais foi emitida uma declaração de conformidade no âmbito de um sistema de certificação da cibersegurança estabelecido nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[33] e cujas referências foram publicadas no *Jornal Oficial da União Europeia* são conformes com os requisitos de cibersegurança estabelecidos no artigo 15.º do presente regulamento, contanto que o certificado de cibersegurança ou a declaração de conformidade ou partes dos mesmos abranjam esses requisitos.

Artigo 43.º

Avaliação da conformidade

1. No respeitante aos sistemas de IA de risco elevado enumerados no anexo III, ponto 1, quando, ao demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, o fornecedor tiver aplicado as normas harmonizadas a que se refere o artigo 40.º, ou, se for caso disso, as especificações comuns a que se refere o artigo 41.º, o fornecedor deve optar por um dos seguintes procedimentos:

   a) O procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI; ou

   b) O procedimento de avaliação da conformidade baseado na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica, com a participação de um organismo notificado, a que se refere o anexo VII.

   Quando, ao demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, o fornecedor não tiver aplicado ou tiver aplicado apenas parcialmente normas harmonizadas a que se refere o artigo 40.º, ou se tais normas harmonizadas não existirem e as especificações comuns a que se refere o artigo 41.º não estiverem disponíveis, o fornecedor deve seguir o procedimento de avaliação da conformidade preconizado no anexo VII.

---

33 Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 1).

Para efeitos do procedimento de avaliação da conformidade a que se refere o anexo VII, o fornecedor pode escolher qualquer um dos organismos notificados. Contudo, se o sistema se destinar a ser colocado em serviço por autoridades competentes em matéria de manutenção da ordem pública, imigração ou asilo, bem como por instituições, órgãos e organismos da UE, a autoridade de fiscalização do mercado a que se refere o artigo 63.º, n.ºs 5 ou 6, consoante o caso, deve atuar como um organismo notificado.

2. Em relação aos sistemas de IA de risco elevado enumerados no anexo III, pontos 2 a 8, e aos sistemas de IA de finalidade geral enumerados no título 1-A, os fornecedores devem seguir o procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI, que não prevê a participação de um organismo notificado.

3. Em relação aos sistemas de IA de risco elevado aos quais são aplicáveis atos jurídicos enumerados no anexo II, secção A, o fornecedor deve seguir o procedimento de avaliação da conformidade aplicável nos termos desses atos jurídicos. Os requisitos estabelecidos no capítulo 2 do presente título aplicam-se a esses sistemas de IA de risco elevado e devem fazer parte dessa avaliação. É igualmente aplicável o disposto no anexo VII, pontos 4.3, 4.4, 4.5, e ponto 4.6, quinto parágrafo.

Para efeitos dessa avaliação, os organismos notificados que tenham sido notificados ao abrigo dos referidos atos jurídicos ficam habilitados a verificar a conformidade dos sistemas de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, contanto que a conformidade desses organismos notificados com os requisitos estabelecidos no artigo 33.º, n.ºs 4, 9 e 10, tenha sido avaliada no contexto do procedimento de notificação previsto nesses atos jurídicos.

Sempre que os atos jurídicos enumerados no anexo II, secção A, permitam ao fabricante do produto renunciar a uma avaliação da conformidade por terceiros, desde que tenha aplicado todas as normas harmonizadas que abrangem os requisitos previstos nesses atos, esse fabricante apenas pode fazer uso de tal opção se tiver também aplicado normas harmonizadas ou, se for caso disso, especificações comuns a que se refere o artigo 41.º que abranjam os requisitos estabelecidos no capítulo 2 do presente título.

4. [suprimido]

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar os anexos VI e VII à luz da evolução técnica.

6. A Comissão fica habilitada a adotar atos delegados para alterar os n.ºs 1 e 2, a fim de sujeitar os sistemas de IA de risco elevado referidos no anexo III, pontos 2 a 8, ao procedimento de avaliação da conformidade referido no anexo VII ou a partes daquele. A Comissão adota esses atos delegados tendo em conta a eficácia do procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI na prevenção ou minimização dos riscos para a saúde e a segurança e a proteção dos direitos fundamentais representados por esses sistemas, bem como a disponibilidade de capacidades e recursos adequados entre os organismos notificados.

Artigo 44.º

Certificados

1. Os certificados emitidos pelos organismos notificados em conformidade com o anexo VII devem ser redigidos numa língua que possa ser facilmente compreendida pelas autoridades competentes do Estado-Membro em que o organismo notificado estiver estabelecido.

2. Os certificados são válidos pelo período neles indicado, que não pode exceder cinco anos. A pedido do fornecedor, a validade de um certificado pode ser prorrogada por novos períodos não superiores a cinco anos, com base numa reavaliação segundo os procedimentos de avaliação da conformidade aplicáveis. Os eventuais aditamentos a um certificado permanecem válidos durante o período de validade do certificado a que dizem respeito.

3. Se verificar que um sistema de IA deixou de cumprir os requisitos estabelecidos no capítulo 2 do presente título, o organismo notificado deve suspender, retirar ou restringir o certificado emitido, tendo em conta o princípio da proporcionalidade, a não ser que o fornecedor do sistema garanta o cumprimento desses requisitos tomando as medidas corretivas necessárias num prazo adequado estabelecido pelo organismo notificado. O organismo notificado deve fundamentar a sua decisão.

Artigo 45.º

Recurso das decisões dos organismos notificados

Deve prever-se um procedimento de recurso das decisões dos organismos notificados.

Artigo 46.º

Obrigações de informação dos organismos notificados

1. Os organismos notificados devem comunicar à autoridade notificadora as seguintes informações:

   a) Certificados da União de avaliação da documentação técnica, todos os suplementos desses certificados, bem como aprovações do sistema de gestão da qualidade emitidos de acordo com os requisitos do anexo VII;

   b) Recusas, restrições, suspensões ou retiradas de certificados da União de avaliação da documentação técnica ou de aprovações de sistemas de gestão da qualidade emitidos em conformidade com os requisitos constantes do anexo VII;

   c) As circunstâncias que afetem o âmbito ou as condições de notificação;

   d) Pedidos de informação que tenham recebido das autoridades de fiscalização do mercado sobre as atividades de avaliação da conformidade;

   e) Se lhes for solicitado, as atividades de avaliação da conformidade realizadas no âmbito da respetiva notificação e quaisquer outras atividades exercidas, nomeadamente atividades transfronteiras e de subcontratação.

2. Cada organismo notificado deve informar os outros organismos notificados sobre:

   a) As aprovações de sistemas de gestão da qualidade que tenha recusado, suspendido ou retirado e, se lhe for pedido, as aprovações que tenha concedido a sistemas de qualidade;

b) Os certificados UE de avaliação da documentação técnica ou quaisquer suplementos dos mesmos que tenha recusado, retirado, suspendido ou restringido de outro modo e, se lhe for pedido, os certificados e/ou suplementos dos mesmos que tenha emitido.

3. Cada organismo notificado deve disponibilizar aos outros organismos notificados que realizam atividades de avaliação da conformidade semelhantes, abrangendo os mesmos sistemas de IA, informações importantes sobre questões relativas aos resultados negativos e, se lhe for pedido, aos resultados positivos de procedimentos de avaliação da conformidade.

4. As obrigações a que se referem os n.ºs 1 a 3 são cumpridas em conformidade com o artigo 70.º.

Artigo 47.º

Derrogação do procedimento de avaliação da conformidade

1. Em derrogação do artigo 43.º e mediante pedido devidamente justificado, qualquer autoridade de fiscalização do mercado pode autorizar a colocação no mercado ou a colocação em serviço de determinados sistemas de IA de risco elevado no território do Estado-Membro em causa, por motivos excecionais de segurança pública ou de proteção da vida e da saúde das pessoas, de proteção do ambiente e de proteção de ativos industriais e infraestruturas essenciais. Essa autorização é concedida por um período limitado, enquanto os procedimentos de avaliação da conformidade necessários estiverem a ser executados, tendo em conta as razões excecionais que justificam a derrogação.
A conclusão desses procedimentos deve ser realizada sem demora injustificada.

1-A. Numa situação de urgência devidamente justificada por motivos excecionais de segurança pública ou em caso de ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares, as autoridades policiais ou as autoridades de proteção civil podem colocar em serviço um sistema de IA de risco elevado específico sem a autorização a se refere o n.º 1, desde que essa autorização seja solicitada durante ou após a utilização sem demora injustificada e, se essa autorização for rejeitada, a sua utilização deve ser suspensa com efeito imediato e todos os resultados dessa utilização devem ser imediatamente rejeitados.

2. A autorização a que se refere o n.º 1 apenas deve ser concedida se a autoridade de fiscalização do mercado concluir que o sistema de IA de risco elevado cumpre os requisitos do capítulo 2 do presente título. A autoridade de fiscalização do mercado deve informar a Comissão e os outros Estados-Membros sobre qualquer autorização concedida nos termos do n.º 1. Esta obrigação não abrange os dados operacionais sensíveis relativos às atividades das autoridades policiais.

3. [suprimido]

4. [suprimido]

5. [suprimido]

6. No caso dos sistemas de IA de risco elevado relacionados com produtos abrangidos pela legislação de harmonização da União a se refere o anexo II, secção A, só são aplicáveis os procedimentos de derrogação de avaliação da conformidade estabelecidos nessa legislação.

Artigo 48.º

Declaração de conformidade UE

1. O fornecedor deve elaborar uma declaração de conformidade UE escrita ou assinada eletronicamente para cada sistema de IA e mantê-la à disposição das autoridades nacionais competentes por um período de dez anos a contar da data de colocação no mercado ou colocação em serviço do sistema de IA. A declaração de conformidade UE deve especificar o sistema de IA para o qual foi elaborada. Deve ser apresentada uma cópia da declaração de conformidade UE às autoridades nacionais competentes, mediante pedido.

2. A declaração de conformidade UE deve mencionar que o sistema de IA de risco elevado em questão cumpre os requisitos estabelecidos no capítulo 2 do presente título.
A declaração de conformidade UE deve conter as informações indicadas no anexo V e ser traduzida para uma língua que possa ser facilmente compreendida pelas autoridades nacionais competentes do(s) Estados-Membro(s) em que o sistema de IA de risco elevado é disponibilizado.

3. Se os sistemas de IA de risco elevado estiverem sujeitos a outra legislação de harmonização da União que também exija uma declaração de conformidade UE, deve ser elaborada uma única declaração de conformidade UE respeitante a todos os atos jurídicos da UE aplicáveis ao sistema de IA de risco elevado. A declaração deve incluir todas as informações necessárias para identificar a legislação de harmonização da União a que diz respeito.

4. Ao elaborar a declaração de conformidade UE, o fornecedor deve assumir a responsabilidade pelo cumprimento dos requisitos estabelecidos no capítulo 2 do presente título. O fornecedor deve manter a declaração de conformidade UE atualizada, consoante necessário.

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar o conteúdo da declaração de conformidade UE preconizado no anexo V, a fim de introduzir elementos que se tornem necessários à luz da evolução técnica.

Artigo 49.º

Marcação de conformidade CE

1. A marcação de conformidade CE está sujeita aos princípios gerais enunciados no artigo 30.º do Regulamento (CE) n.º 765/2008.

2. A marcação CE deve ser aposta de modo visível, legível e indelével em sistemas de IA de risco elevado. Caso a natureza do sistema de IA de risco elevado não permita ou não garanta essas características da marcação, esta deve ser aposta na embalagem ou na documentação que acompanha o sistema, conforme mais adequado.

3. Quando aplicável, a marcação CE deve ser seguida pelo número de identificação do organismo notificado responsável pelos procedimentos de avaliação da conformidade estabelecidos no artigo 43.º. O número de identificação deve ser igualmente indicado em qualquer material promocional que mencione que o sistema de IA de risco elevado cumpre os requisitos aplicáveis à marcação CE.

Artigo 50.º

[suprimido]

Artigo 51.º

Registo dos operadores pertinentes e dos sistemas de IA de risco elevado enumerados no anexo III

1. Antes da colocação no mercado ou da colocação em serviço de um sistema de IA de risco elevado enumerado no anexo III, com exceção dos sistemas de IA de risco elevado referidos no anexo III, pontos 1, 6 e 7, nos domínios da manutenção da ordem pública e da gestão da migração, do asilo e do controlo das fronteiras, e dos sistemas de IA de risco elevado referidos no anexo III, ponto 2, o fornecedor e, se for caso disso, o mandatário devem registar-se na base de dados da UE a que se refere o artigo 60.º. O fornecedor ou, se for caso disso, o mandatário deve também registar os seus sistemas nessa base de dados.

2. Antes de utilizarem um sistema de IA de risco elevado enumerado no anexo III, os utilizadores de sistemas de IA de risco elevado que sejam autoridades, agências ou organismos públicos, ou entidades que atuem em seu nome, devem registar-se na base de dados da UE a que se refere o artigo 60.º e selecionar o sistema que tencionam utilizar.

   As obrigações estabelecidas no parágrafo anterior não se aplicam às autoridades policiais, às autoridades, agências ou organismos de controlo das fronteiras, de imigração ou de asilo, às autoridades, agências ou organismos que utilizam sistemas de IA de risco elevado a que se refere o anexo III, ponto 2, nem às entidades que atuam em seu nome.

TÍTULO IV

OBRIGAÇÕES DE TRANSPARÊNCIA APLICÁVEIS AOS FORNECEDORES E UTILIZADORES DE DETERMINADOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Artigo 52.º

Obrigações de transparência aplicáveis aos fornecedores e utilizadores de determinados sistemas de inteligência artificial

1. Os fornecedores devem assegurar que os sistemas de IA destinados a interagir com pessoas singulares sejam concebidos e desenvolvidos de maneira que as pessoas singulares sejam informadas de que estão a interagir com um sistema de IA, salvo se tal se revelar óbvio do ponto de vista de uma pessoa singular razoavelmente informada, atenta e advertida, tendo em conta as circunstâncias e o contexto de utilização. Esta obrigação não se aplica a sistemas de IA legalmente autorizados para detetar, prevenir, investigar e reprimir infrações penais, desde que salvaguarde adequadamente os direitos e as liberdades de terceiros, salvo se esses sistemas estiverem disponíveis ao público para denunciar uma infração penal.

2. Os utilizadores de um sistema de categorização biométrica devem informar sobre o funcionamento do sistema as pessoas a ele expostas. Esta obrigação não se aplica a sistemas de IA usados para categorização biométrica que sejam legalmente autorizados para detetar, prevenir e investigar infrações penais, desde que salvaguarde adequadamente os direitos e as liberdades de terceiros.

2-A. Os utilizadores de um sistema de reconhecimento de emoções devem informar sobre o funcionamento do sistema as pessoas a ele expostas. Esta obrigação não se aplica a sistemas de IA usados para reconhecimento de emoções que sejam legalmente autorizados para detetar, prevenir e investigar infrações penais, sob reserva de garantias adequadas para os direitos e liberdades de terceiros.

3. Os utilizadores de um sistema de IA que gera ou manipula conteúdos de imagem, áudio ou vídeo que sejam consideravelmente semelhantes a pessoas, objetos, locais ou outras entidades ou acontecimentos reais e que, falsamente, pareçam ser autênticos e verdadeiros a uma pessoa ("falsificação profunda") devem divulgar que o conteúdo foi gerado ou manipulado artificialmente.

Contudo, o primeiro parágrafo não se aplica se a utilização for legalmente autorizada para detetar, prevenir, investigar e reprimir infrações penais ou se o conteúdo fizer parte de uma obra ou de um programa aparentemente criativo, satírico, artístico ou fictício, desde que salvaguarde adequadamente os direitos e as liberdades de terceiros.

3-A. As informações a que se referem os n.ºs 1 a 3 são fornecidas às pessoas singulares de forma clara e distinguível, o mais tardar aquando da primeira interação ou exposição.

4. Os n.ºs 1, 2, 2-A, 3 e 3-A não afetam os requisitos e as obrigações estabelecidos no título III do presente regulamento e não prejudicam outras obrigações de transparência aplicáveis aos utilizadores de sistemas de IA estabelecidas na legislação da União ou nacional.

TÍTULO V

MEDIDAS DE APOIO À INOVAÇÃO

Artigo 53.º

Ambientes de testagem da regulamentação da inteligência artificial

-1-A. As autoridades nacionais competentes podem criar ambientes de testagem da regulamentação da inteligência artificial para o desenvolvimento, treino, testagem e validação de sistemas de IA inovadores, sob a supervisão, a orientação e o apoio diretos da autoridade nacional competente, antes de esses sistemas serem colocados no mercado ou colocados em serviço. Esses ambientes de testagem da regulamentação podem incluir testes em condições reais supervisionadas pelas autoridades nacionais competentes.

-1-B. [suprimido]

-1-C. Se for caso disso, as autoridades nacionais competentes devem cooperar com outras autoridades pertinentes e podem permitir a participação de outros intervenientes no ecossistema de IA.

-1-D. O presente artigo não afeta outros ambientes de testagem da regulamentação estabelecidos ao abrigo da legislação nacional ou da União, nomeadamente nos casos em que os produtos ou serviços neles testados estejam associados à utilização de sistemas de IA inovadores. Os Estados-Membros asseguram um nível adequado de cooperação entre as autoridades que supervisionam esses outros ambientes de testagem e as autoridades nacionais competentes.

1. [suprimido]

1-A. [suprimido]

1-B. A criação de ambientes de testagem da regulamentação da IA ao abrigo do presente regulamento visa contribuir para um ou mais dos seguintes objetivos:

a) Promover a inovação e a competitividade e facilitar o desenvolvimento de um ecossistema de IA;
b) Facilitar e acelerar o acesso dos sistemas de IA ao mercado da União, em especial quando fornecidos por pequenas e médias empresas (PME), incluindo empresas em fase de arranque;
c) Melhorar a segurança jurídica e contribuir para a partilha de boas práticas através da cooperação com as autoridades envolvidas no ambiente de testagem da regulamentação da IA, com vista a assegurar o futuro cumprimento do presente regulamento e, se for caso disso, de outra legislação da União e dos Estados-Membros;
d) Contribuir para uma aprendizagem regulamentar baseada em dados concretos.

2. [suprimido]

2-A. O acesso aos ambientes de testagem da regulamentação da IA está aberto a qualquer fornecedor ou potencial fornecedor de um sistema de IA que cumpra os critérios de elegibilidade e seleção a que se refere o n.º 6, alínea a), e que tenha sido selecionado pelas autoridades nacionais competentes na sequência do procedimento de seleção a que se refere o n.º 6, alínea b). Os fornecedores ou potenciais fornecedores podem também apresentar pedidos em parceria com utilizadores ou quaisquer outros terceiros pertinentes.

A participação no ambiente de testagem da regulamentação da IA é limitada a um período adequado à complexidade e dimensão do projeto. Esse período pode ser prorrogado pela autoridade nacional competente.

A participação no ambiente de testagem da regulamentação da IA baseia-se num plano específico a que se refere o n.º 6 do presente artigo, que é acordado entre o(s) participante(s) e a autoridade ou autoridades nacionais competentes, conforme aplicável.

3. A participação nos ambientes de testagem da regulamentação da IA não afeta os poderes de supervisão e de correção das autoridades que supervisionam o ambiente de testagem. Essas autoridades exercem os seus poderes de supervisão de forma flexível, dentro dos limites da legislação aplicável, utilizando os seus poderes discricionários quando aplicam disposições jurídicas a um projeto específico de ambiente de testagem da IA, com o objetivo de apoiar a inovação no domínio da IA na União.

Desde que o(s) participante(s) respeite(m) o plano do ambiente de testagem e os termos e condições da sua participação, tal como referido no n.º 6, alínea c), e siga(m) de boa-fé as orientações dadas pelas autoridades, as autoridades não aplicam coimas por infração à legislação aplicável da União ou dos Estados-Membros relativa ao sistema de IA supervisionado no ambiente de testagem, incluindo as disposições do presente regulamento.

4. Os participantes continuam a ser responsáveis, nos termos da legislação aplicável da União e dos Estados-Membros em matéria de responsabilidade, por todos os danos causados no decurso da sua participação num ambiente de testagem da regulamentação da IA.

4-A. A pedido do fornecedor ou potencial fornecedor do sistema de IA, a autoridade nacional competente apresenta, se for caso disso, uma prova escrita das atividades realizadas com êxito no ambiente de testagem. A autoridade nacional competente também apresenta um relatório de saída que descreva pormenorizadamente as atividades realizadas no ambiente de testagem e as respetivas conclusões e resultados de aprendizagem. Essas provas escritas e relatórios de saída podem ser tidos em conta pelas autoridades de fiscalização do mercado ou pelos organismos notificados, consoante o caso, no contexto de procedimentos de avaliação da conformidade ou de atividades de fiscalização do mercado.

Sob reserva das disposições em matéria de confidencialidade previstas no artigo 70.º com o acordo dos participantes no ambiente de testagem, a Comissão Europeia e o Comité para a Inteligência Artificial estão autorizados a aceder aos relatórios de saída e têm os mesmos em conta, se for caso disso, no exercício das suas funções ao abrigo do presente regulamento. Se tanto o participante como a autoridade nacional competente derem o seu acordo explícito, o relatório de saída pode ser disponibilizado ao público através da plataforma única de informação a que se refere o artigo 55.º, n.º 3, alínea b).

4-B. Os ambientes de testagem da regulamentação da IA são concebidos e aplicados de forma a facilitar, se for caso disso, a cooperação transfronteiriça entre as autoridades nacionais competentes.

5. As autoridades nacionais competentes disponibilizam ao público relatórios anuais sobre a aplicação de ambientes de testagem da regulamentação da IA, incluindo boas práticas, ensinamentos retirados e recomendações sobre a sua configuração e, se for caso disso, sobre a aplicação do presente regulamento e de outra legislação da União supervisionada no ambiente de testagem. Esses relatórios anuais devem ser apresentados ao Comité para a Inteligência Artificial, que disponibiliza ao público um resumo de todas as boas práticas, ensinamentos retirados e recomendações. Essa obrigação de disponibilizar ao público os relatórios anuais não abrange dados operacionais sensíveis relacionados com as atividades das autoridades policias, de controlo das fronteiras, de imigração ou de asilo. A Comissão e o Comité para a Inteligência Artificial têm em conta, se for caso disso, os relatórios anuais no exercício das suas funções ao abrigo do presente regulamento.

5-B. A Comissão assegura que as informações sobre ambientes de testagem da regulamentação da IA, inclusive sobre os ambientes criados ao abrigo do presente artigo, estão disponíveis através da plataforma única de informação a que se refere o artigo 55.º, n.º 3, alínea b).

6. As modalidades e as condições para a criação e o funcionamento dos ambientes de testagem da regulamentação da IA ao abrigo do presente regulamento são adotadas através de atos de execução em conformidade com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

As modalidades e condições apoiam, na medida do possível, a flexibilidade para que as autoridades nacionais competentes estabeleçam e operem os seus ambientes de testagem da regulamentação da IA e promovam a inovação e a aprendizagem regulamentar, e têm especialmente em conta as circunstâncias especiais e as capacidades das PME participantes, incluindo as empresas em fase de arranque.

Esses atos de execução incluem princípios fundamentais comuns sobre as seguintes questões:

a) A elegibilidade e a seleção para a participação no ambiente de testagem da regulamentação da IA;
b) O procedimento para a candidatura, participação, monitorização, saída e cessação do ambiente de testagem da regulamentação da IA, incluindo o plano do ambiente de testagem e o relatório de saída;
c) Os termos e as condições aplicáveis aos participantes.

7. Sempre que ponderem autorizar a testagem em condições reais supervisionada no âmbito de um ambiente de testagem da regulamentação da IA criado ao abrigo do presente artigo, as autoridades nacionais competentes devem acordar especificamente com os participantes os termos e condições dessa testagem e, em especial, as salvaguardas adequadas com vista a proteger os direitos fundamentais, a saúde e a segurança. Se for caso disso, cooperam com outras autoridades nacionais competentes com vista a assegurar práticas coerentes em toda a União.

Artigo 54.º

Tratamento adicional de dados pessoais para efeitos de desenvolvimento de certos sistemas de inteligência artificial de interesse público no ambiente de testagem da regulamentação da inteligência artificial

1. No ambiente de testagem da regulamentação da IA, os dados pessoais legalmente recolhidos para outras finalidades podem ser tratados com vista a desenvolver, testar e treinar sistemas de IA inovadores no ambiente de testagem nas seguintes condições:

   a) Os sistemas de IA inovadores devem ser desenvolvidos para salvaguarda de um interesse público substancial por uma autoridade pública ou outra pessoa singular ou coletiva regida pelo direito público ou pelo direito privado e num ou mais dos seguintes domínios:

      i) [suprimido]

      ii) segurança e saúde públicas, nomeadamente a prevenção, o controlo e o tratamento de doenças e a melhoria dos sistemas de saúde;

      iii) proteção e melhoria da qualidade do ambiente, nomeadamente a transição ecológica, a atenuação das alterações climáticas e a adaptação às mesmas;

      iv) sustentabilidade energética, transportes e mobilidade;

      v) eficiência e qualidade da administração pública e dos serviços públicos;

      vi) cibersegurança e resiliência das infraestruturas críticas.

   b) Os dados tratados são necessários para cumprir um ou vários dos requisitos referidos no título III, capítulo 2, caso esses requisitos não possam ser eficazmente cumpridos mediante tratamento de dados anonimizados, sintéticos ou outros dados não pessoais;

c) Existem mecanismos de controlo eficazes para identificar os riscos elevados para os direitos e as liberdades dos titulares dos dados, tal como referido no artigo 35.º do Regulamento (UE) 2016/679 e no artigo 39.º do Regulamento (UE) 2018/1725, que possam surgir durante a experimentação no ambiente de testagem, bem como um mecanismo de resposta para atenuar prontamente esses riscos e, se necessário, interromper o tratamento dos dados;

d) Todos os dados pessoais a tratar no contexto do ambiente de testagem se encontram num ambiente de tratamento de dados funcionalmente separado, isolado e protegido sob o controlo dos participantes, sendo apenas acessíveis a pessoas autorizadas;

e) Nenhuns dados pessoais tratados são transmitidos, transferidos ou acedidos, de outro modo, por terceiros que não sejam participantes no ambiente de testagem, a menos que essa divulgação ocorra em conformidade com o Regulamento (UE) 2016/679 ou, se aplicável, com o Regulamento 2018/725, e todos os participantes tenham dado o seu acordo;

f) Nenhum tratamento de dados pessoais no contexto do ambiente de testagem afeta a aplicação dos direitos dos titulares dos dados previstos na legislação da União em matéria de proteção de dados pessoais, nomeadamente no artigo 22.º do Regulamento (UE) 2016/679 e no artigo 24.º do Regulamento (UE) 2018/1725;

g) Todos os dados pessoais tratados no contexto do ambiente de testagem são protegidos por meio de medidas técnicas e organizativas adequadas e apagados assim que a participação no ambiente de testagem terminar ou que os dados pessoais atingirem o fim do respetivo período de conservação;

h) Os registos do tratamento de dados pessoais no contexto do ambiente de testagem são mantidos durante a participação no ambiente de testagem, salvo disposição em contrário na legislação da União ou nacional;

i) É mantida, juntamente com os resultados dos testes, uma descrição completa e pormenorizada do processo e da lógica subjacentes ao treino, ao teste e à validação do sistema de IA como parte da documentação técnica prevista no anexo IV;

j) Uma breve síntese do projeto de IA desenvolvido no ambiente de testagem, incluindo os seus objetivos e resultados esperados, é publicada no sítio Web das autoridades competentes. Esta obrigação não abrange dados operacionais sensíveis relacionados com as atividades das autoridades policias, de controlo das fronteiras, de imigração ou de asilo.

1-A. Para efeitos de prevenção, investigação, deteção ou repressão de infrações penais, ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas, sob o controlo e a responsabilidade das autoridades policiais, o tratamento de dados pessoais em ambientes de testagem da regulamentação da IA baseia-se em legislação específica de um Estado-Membro ou da União e está sujeito às mesmas condições cumulativas referidas no n.º 1.

2. O n.º 1 não prejudica a legislação da União nem dos Estados-Membros que estabelece a base para o tratamento de dados pessoais necessário para efeitos de desenvolvimento, testagem e treino de sistemas de IA inovadores ou qualquer outra base jurídica, em conformidade com a legislação da União em matéria de proteção de dados pessoais.

Artigo 54.º-A

Testagem de sistemas de IA de risco elevado em condições reais fora dos ambientes de testagem da regulamentação da IA

1. A testagem de sistemas de IA em condições reais fora dos ambientes de testagem da regulamentação da IA pode ser realizada por fornecedores ou potenciais fornecedores de sistemas de IA de risco elevado enumerados no anexo III, em conformidade com as disposições do presente artigo e com o plano de testagem em condições reais a que se refere o presente artigo.

Os elementos pormenorizados do plano de testagem em condições reais são especificados em atos de execução adotados pela Comissão de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

Esta disposição não prejudica a legislação da União nem dos Estados-Membros relativa à testagem em condições reais de sistemas de IA de risco elevado relacionados com produtos abrangidos pela legislação enumerada no anexo II.

2. Os fornecedores ou potenciais fornecedores podem testar os sistemas de IA de risco elevado a que se refere o anexo III em condições reais em qualquer momento antes da colocação no mercado ou da colocação em serviço do sistema de IA, isoladamente ou em parceria com um ou mais potenciais utilizadores.

3. A testagem de sistemas de IA de risco elevado em condições reais ao abrigo do presente artigo não prejudica a análise ética que possa ser exigida pela legislação nacional ou da União.

4. Os fornecedores ou potenciais fornecedores só podem realizar a testagem em condições reais se estiverem preenchidas todas as seguintes condições:

a) O fornecedor ou potencial fornecedor elaborou um plano de testagem em condições reais e apresentou-o à autoridade de fiscalização do mercado do(s) Estado(s)-Membro(s) onde a testagem deve realizar-se em condições reais;

b) A autoridade de fiscalização do mercado do(s) Estado(s)-Membro(s) onde a testagem deve realizar-se em condições reais não se opôs à testagem no prazo de 30 dias após a sua apresentação;

c) O fornecedor ou potencial fornecedor, com exceção dos sistemas de IA de risco elevado referidos no anexo III, pontos 1, 6 e 7, nos domínios da manutenção da ordem pública e da gestão da migração, do asilo e do controlo das fronteiras, e dos sistemas de IA de risco elevado referidos no anexo III, ponto 2, registou a testagem em condições reais na base de dados da UE a que se refere o artigo 60.º, n.º 5-A, com um número único de identificação a nível da União, e as informações especificadas no anexo VIII-A;

d) O fornecedor ou potencial fornecedor que realiza a testagem em condições reais está estabelecido na União ou nomeou um representante legal para a testagem em condições reais que está estabelecido na União;

e) Os dados recolhidos e tratados para efeitos de testagem em condições reais não são transferidos para países fora da União, a menos que a sua transferência e tratamento proporcionem garantias equivalentes às previstas na legislação da União;

f) A testagem em condições reais não dura mais tempo do que o necessário para atingir os seus objetivos e, em caso algum, não excede 12 meses;

g) As pessoas pertencentes a grupos vulneráveis devido à sua idade ou deficiência física ou mental estão devidamente protegidas;

h) [suprimido]

i) Sempre que um fornecedor ou potencial fornecedor organiza a testagem em condições reais em colaboração com um ou mais potenciais utilizadores, estes últimos foram informados de todos os aspetos da testagem que são pertinentes para a sua decisão de participar e receberam as instruções pertinentes sobre a forma de utilizar o sistema de IA a que se refere o artigo 13.º; O prestador ou potencial fornecedor e o(s) utilizador(es) celebram um acordo que especifique as suas funções e responsabilidades, a fim de assegurar o cumprimento das disposições relativas à testagem em condições reais nos termos do presente regulamento e de outra legislação aplicável da União e dos Estados-Membros;

j) Os participantes da testagem em condições reais deram o seu consentimento informado em conformidade com o artigo 54.º-B ou, no caso das autoridades policiais, se a obtenção do consentimento informado impedir que o sistema de IA seja testado, a testagem propriamente dita e os resultados da testagem em condições reais não têm um efeito negativo sobre o participante da testagem;

k) A testagem em condições reais é efetivamente supervisionada pelo fornecedor ou potencial fornecedor e pelo(s) utilizador(es) com pessoas devidamente qualificadas no domínio em causa e com a capacidade, a formação e a autoridade necessárias para desempenhar as respetivas funções;

l) As previsões, recomendações ou decisões do sistema de IA podem ser efetivamente revertidas ou ignoradas.

5. Os participantes da testagem em condições reais, ou o seu representante legalmente autorizado, consoante o caso, podem, sem que daí decorra qualquer prejuízo e sem terem que apresentar qualquer justificação, retirar-se da testagem a qualquer momento retirando, para tal, o seu consentimento informado. A retirada do consentimento informado não afeta as atividades já realizadas nem a utilização dos dados obtidos com base no consentimento informado antes da sua retirada.

6. Qualquer incidente grave identificado durante a testagem em condições reais é comunicado à autoridade nacional de fiscalização do mercado em conformidade com o artigo 62.º do presente regulamento. O fornecedor ou potencial fornecedor deve adotar medidas de atenuação imediatas ou, na sua falta, suspender a testagem em condições reais até que essa atenuação tenha lugar ou, caso contrário, cessar a testagem. O fornecedor ou potencial fornecedor deve estabelecer um procedimento para a recolha rápida do sistema de IA após a cessação da testagem em condições reais.

7. Os fornecedores ou potenciais fornecedores devem notificar a autoridade nacional de fiscalização do mercado do(s) Estado(s) –Membro(s) onde a testagem deve realizar-se em condições reais da suspensão ou cessação da testagem em condições reais e dos resultados finais.

8. Os fornecedores ou potenciais fornecedores são responsáveis, nos termos da legislação aplicável da União e dos Estados-Membros em matéria de responsabilidade, por quaisquer danos causados no decurso da sua participação numa testagem em condições reais.

Artigo 54.º-B

Consentimento informado para participar em testagens em condições reais fora dos ambientes de testagem da regulamentação da IA

1. Para efeitos de testagem em condições reais nos termos do artigo 54.º-A, o consentimento informado deve ser dado livremente pelo participante da testagem antes da sua participação nessa testagem e depois de lhe terem sido devidamente prestadas informações concisas, claras, pertinentes e compreensíveis sobre:

i) a natureza e os objetivos da testagem em condições reais e os eventuais inconvenientes que possam estar ligados à sua participação;

ii) as condições em que a testagem em condições reais deve realizar-se, incluindo a duração prevista da sua participação na testagem;

iii) os direitos e garantias relativos à participação, em particular o direito de recusar a participação na testagem em condições reais e o direito de se retirar da mesma em qualquer altura, sem que daí decorra qualquer prejuízo e sem ter de justificar tal decisão;

iv) as modalidades para solicitar que as previsões, recomendações ou decisões do sistema de IA sejam revertidas ou ignoradas;

v) o número único de identificação a nível da União da testagem em condições reais, em conformidade com o artigo 54.º-A, n.º 4-C, e os dados de contacto do fornecedor, ou do seu representante legal, junto do qual podem ser obtidas mais informações.

2. O consentimento informado deve ser datado e documentado e deve ser dada uma cópia ao participante da testagem ou ao seu representante legal.

Artigo 55.º

Medidas de apoio aos operadores, em especial as PME, incluindo empresas em fase de arranque

1. Os Estados-Membros devem empreender as seguintes ações:

a) Proporcionar às PME, incluindo às empresas em fase de arranque, acesso prioritário aos ambientes de testagem da regulamentação da IA, desde que cumpram os critérios de elegibilidade e de seleção;

b) Organizar atividades de sensibilização e de formação específicas sobre a aplicação do presente regulamento adaptadas às necessidades das PME, incluindo das empresas em fase de arranque, e, conforme adequado, das autoridades públicas locais;

c) Se for caso disso, criar um canal específico para comunicação com as PME, incluindo as empresas em fase de arranque e, conforme adequado, as autoridades públicas locais, com o intuito de prestar aconselhamento e responder a consultas sobre a aplicação do presente regulamento, nomeadamente no que diz respeito à participação em ambientes de testagem da regulamentação da IA.

2. Os interesses e as necessidades específicas dos fornecedores que são PME, incluindo as empresas em fase de arranque, devem ser tidos em conta aquando da fixação das taxas a pagar pela avaliação da conformidade nos termos do artigo 43.º, reduzindo essas taxas proporcionalmente à sua dimensão, à dimensão do mercado e demais indicadores pertinentes.

3. A Comissão empreende as seguintes ações:

(a) A pedido do Comité para a Inteligência Artificial, fornecer modelos normalizados para os domínios abrangidos pelo presente regulamento;

(b) Desenvolver e manter uma plataforma única de informação que forneça informações de fácil utilização relacionadas com o presente regulamento a todos os operadores em toda a União;

(c) Organizar campanhas de comunicação adequadas para sensibilizar para as obrigações decorrentes do presente regulamento;

(d) Avaliar e promover a convergência das boas práticas nos processos de adjudicação de contratos públicos em relação aos sistemas de IA.

Artigo 55.º-A

Derrogações aplicáveis a operadores específicos

1. As obrigações estabelecidas no artigo 17.º do presente regulamento não se aplicam às microempresas na aceção do artigo 2.º, n.º 3, do anexo da Recomendação 2003/361/CE da Comissão relativa à definição de micro, pequenas e médias empresas, desde que essas empresas não tenham empresas parceiras ou empresas associadas na aceção do artigo 3.º do mesmo anexo.

2. O n.º 1 não pode ser interpretado no sentido de isentar esses operadores do cumprimento de quaisquer outros requisitos e obrigações estabelecidos no presente regulamento, incluindo os estabelecidos nos artigos 9.º, 61.º e 62.º.

3. Os requisitos e obrigações para sistemas de IA de finalidade geral estabelecidos no artigo 4.º-B não se aplicam às micro, pequenas e médias empresas, desde que essas empresas não tenham empresas parceiras ou empresas associadas na aceção do artigo 3.º do anexo da Recomendação 2003/361/CE da Comissão relativa à definição de micro, pequenas e médias empresas.

TÍTULO VI

GOVERNAÇÃO

CAPÍTULO 1

COMITÉ EUROPEU PARA A INTELIGÊNCIA ARTIFICIAL

Artigo 56.º

Criação e estrutura do Comité Europeu para a Inteligência Artificial

1. É criado um Comité Europeu para a Inteligência Artificial (adiante designado por "Comité").

2. O Comité é composto por um representante de cada Estado-Membro. A Autoridade Europeia para a Proteção de Dados participa na qualidade de observador. A Comissão participa igualmente nas reuniões do Comité, mas não participa nas votações.

   O Comité pode convidar para as reuniões, caso a caso, outras autoridades, organismos ou peritos nacionais e da União, sempre que as questões debatidas sejam pertinentes para os mesmos.

2-A. Cada representante é designado pelo respetivo Estado-Membro por um período de três anos, renovável uma vez.

2-AA. Os Estados-Membros asseguram que os seus representantes no Comité:

   i) dispõem das competências e poderes pertinentes no seu Estado-Membro, de modo a contribuir ativamente para o desempenho das funções do Comité a que se refere o artigo 58.º;

   ii) são designados como ponto de contacto único para o Comité e, se for caso disso, tendo em conta as necessidades dos Estados-Membros, como ponto de contacto único para as partes interessadas;

iii) estão habilitados a facilitar a coerência e a coordenação entre as autoridades nacionais competentes nos respetivos Estados-Membros no que diz respeito à aplicação do presente regulamento, nomeadamente através da recolha de dados e informações pertinentes para efeitos do exercício das suas funções no Comité.

3. Os representantes designados dos Estados-Membros adotam o regulamento interno do Comité por maioria de dois terços.

O regulamento interno estabelece, em especial, os procedimentos para o processo de seleção, a duração do mandato e as especificações das funções do presidente, as modalidades de votação e a organização das atividades do Comité e dos seus subgrupos.

O Comité deve criar um subgrupo permanente que sirva de plataforma para as partes interessadas o aconselharem sobre todas as questões relacionadas com a aplicação do presente regulamento, inclusive sobre a preparação de atos de execução e atos delegados. Para o efeito, devem ser convidadas a participar neste subgrupo as organizações que representam os interesses dos fornecedores e utilizadores de sistemas de IA, incluindo PME e empresas em fase de arranque, bem como organizações da sociedade civil, representantes das pessoas afetadas, investigadores, organizações de normalização, organismos notificados, laboratórios e instalações de ensaio e experimentação. O Comité cria dois subgrupos permanentes a fim de proporcionar uma plataforma de cooperação e intercâmbio entre as autoridades de fiscalização do mercado e as autoridades notificadoras sobre questões relacionadas com a fiscalização do mercado e os organismos notificados, respetivamente.

O Comité pode constituir outros subgrupos permanentes ou temporários consoante adequado para efeitos da análise de questões específicas. Se for caso disso, as partes interessadas a que se refere o parágrafo anterior podem ser convidadas para esses subgrupos ou para reuniões específicas desses subgrupos na qualidade de observadores.

3-A. O Comité deve estar organizado e funcionar de modo a salvaguardar a objetividade e a imparcialidade das suas atividades.

4. O Comité é presidido por um dos representantes dos Estados-Membros. A pedido do presidente, a Comissão convoca as reuniões e prepara a ordem de trabalhos de acordo com as funções do Comité nos termos do presente regulamento e com o seu regulamento interno. A Comissão presta apoio administrativo e analítico às atividades do Comité nos termos com o presente regulamento.

Artigo 57.º

[suprimido]

Artigo 58.º

Funções do Comité

O Comité presta aconselhamento e assistência à Comissão e aos Estados-Membros, a fim de facilitar a aplicação coerente e eficaz do presente regulamento. Para o efeito, o Comité pode, nomeadamente:

a) Recolher e partilhar conhecimentos técnicos e regulamentares e boas práticas entre Estados-Membros;

b) Contribuir para a harmonização das práticas administrativas nos Estados-Membros, nomeadamente no que diz respeito à derrogação dos procedimentos de avaliação da conformidade a que se refere o artigo 47.º, ao funcionamento dos ambientes de testagem da regulamentação e à testagem em condições reais a que se referem os artigo 53.º, 54.º e 54.º-A;

c) A pedido da Comissão ou por sua própria iniciativa, emitir recomendações e pareceres escritos sobre quaisquer matérias pertinentes relacionadas com a execução do presente regulamento e com a sua aplicação coerente e eficaz, inclusive:

   i) sobre especificações técnicas ou normas existentes relativas aos requisitos estabelecidos no título III, capítulo 2,

   ii) sobre a utilização de normas harmonizadas ou especificações comuns a que se referem os artigos 40.º e 41.º,

iii) sobre a preparação de documentos de orientação, nomeadamente as orientações relativas à fixação de coimas a que se refere o artigo 71.º;

d) Aconselhar a Comissão sobre a eventual necessidade de alterar o anexo III, em conformidade com os artigos 4.º e 7.º, tendo em conta os dados pertinentes disponíveis e os últimos desenvolvimentos tecnológicos;

e) Aconselhar a Comissão durante a preparação de atos delegados ou de atos de execução nos termos do presente regulamento;

f) Cooperar, conforme adequado, com os organismos, grupos de peritos e redes pertinentes da UE, em especial nos domínios da segurança dos produtos, da cibersegurança, da concorrência, dos serviços digitais e de comunicação social, dos serviços financeiros, das criptomoedas, da defesa dos consumidores, dos dados e da proteção dos direitos fundamentais;

g) Contribuir e prestar aconselhamento pertinente à Comissão na elaboração das orientações a que se refere o artigo 58.º-A ou solicitar a elaboração dessas orientações;

h) Apoiar o trabalho das autoridades de fiscalização do mercado e, em cooperação com as autoridades de fiscalização do mercado em causa e sob reserva do acordo destas, promover e apoiar investigações de fiscalização do mercado transfronteiriças, nomeadamente no que diz respeito ao aparecimento de riscos de natureza sistémica que possam advir dos sistemas de IA;

i) Contribuir para a avaliação das necessidades de formação do pessoal dos Estados-Membros envolvido na aplicação do presente regulamento;

j) Aconselhar a Comissão em relação a questões internacionais em matéria de inteligência artificial.

CAPÍTULO 1-A

ORIENTAÇÕES DA COMISSÃO

Artigo 58.º-A

Orientações da Comissão sobre a aplicação do presente regulamento

1. A pedido dos Estados-Membros ou do Comité, ou por sua própria iniciativa, a Comissão emite orientações sobre a aplicação prática do presente regulamento e, em especial, sobre:

   i) a aplicação dos requisitos a que se referem os artigos 8.º a 15.º;

   ii) as práticas proibidas a que se refere o artigo 5.º;

   iii) a aplicação prática das disposições relativas a modificações substanciais;

   iv) a aplicação prática das condições uniformes a que se refere o artigo 6.º, n.º 3, incluindo exemplos em relação aos sistemas de IA de risco elevado referidos no anexo III;

   v) a aplicação prática das obrigações de transparência estabelecidas no artigo 52.º;

   vi) a relação do presente regulamento com outra legislação pertinente da União, nomeadamente no que diz respeito à coerência na sua aplicação.

Ao emitir essas orientações, a Comissão deve prestar especial atenção às necessidades das PME, incluindo as empresas em fase de arranque, das autoridades públicas locais e dos setores mais suscetíveis de serem afetados pelo presente regulamento.

CAPÍTULO 2

AUTORIDADES NACIONAIS COMPETENTES

Artigo 59.º

Designação das autoridades nacionais competentes

1. [suprimido]

2. Cada Estado-Membro deve criar ou designar pelo menos uma autoridade notificadora e pelo menos uma autoridade de fiscalização do mercado para efeitos do presente regulamento como autoridades nacionais competentes. Essas autoridades nacionais competentes devem estar organizadas de modo que garanta os princípios da objetividade e da imparcialidade das suas atividades e funções. Desde que esses princípios sejam respeitados, tais atividades e funções podem ser desempenhadas por uma ou várias autoridades designadas, de acordo com as necessidades organizativas do Estado-Membro.

3. Os Estados-Membros devem informar a Comissão da sua designação ou designações.

4. Os Estados-Membros asseguram que as autoridades nacionais competentes disponham dos recursos financeiros, do equipamento técnico e dos recursos humanos altamente qualificados adequados para exercerem eficazmente as funções que lhes incumbem nos termos do presente regulamento.

5. Até *[um ano após a entrada em vigor do presente regulamento]* e, posteriormente, seis meses antes do termo do prazo a que se refere o artigo 84.º, n.º 2, os Estados-Membros informam a Comissão sobre a situação dos recursos financeiros, do equipamento técnico e dos recursos humanos ao dispor das autoridades nacionais competentes, incluindo uma avaliação da sua adequação. A Comissão transmite essas informações ao Comité para apreciação e eventuais recomendações.

6. A Comissão facilita o intercâmbio de experiências entre as autoridades nacionais competentes.

7. As autoridades nacionais competentes podem prestar aconselhamento sobre a execução do presente regulamento, nomeadamente aconselhamento adaptado aos fornecedores que são PME, incluindo as empresas em fase de arranque. Sempre que as autoridades nacionais competentes pretendam fornecer orientações e prestar aconselhamento em relação a um sistema de IA em domínios abrangidos por outra legislação da União, as autoridades nacionais competentes ao abrigo dessa legislação da União devem ser consultadas, conforme adequado. Os Estados-Membros também podem criar um ponto de contacto central para a comunicação com os operadores.

8. Sempre que as instituições, órgãos e organismos da União se insiram no âmbito do presente regulamento, a Autoridade Europeia para a Proteção de Dados deve atuar como a autoridade competente para o controlo dos mesmos.

TÍTULO VII

BASE DE DADOS DA UE RELATIVA AOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO ENUMERADOS NO ANEXO III

Artigo 60.º

Base de dados da UE relativa aos sistemas de inteligência artificial de risco elevado enumerados no anexo III

1. A Comissão, em colaboração com os Estados-Membros, cria e mantém uma base de dados da UE que contenha as informações referidas no n.º 2 relativas aos operadores pertinentes e aos sistemas de IA de risco elevado enumerados no anexo III que estejam registados em conformidade com os artigos 51.º e 54.º-A. Ao estabelecer as especificações funcionais dessa base de dados, a Comissão deve consultar o Comité para a Inteligência Artificial.

2. Os dados enumerados no anexo VIII, parte I, são introduzidos na base de dados da UE pelos fornecedores, mandatários e utilizadores pertinentes, consoante o caso, aquando do seu registo. Os dados enumerados no anexo VIII, parte II, pontos 1 a 11, são introduzidos na base de dados da UE pelos fornecedores ou, se aplicável, pelo mandatário, em conformidade com o artigo 51.º. Os dados referidos no anexo VIII, parte II, ponto 12, são gerados automaticamente pela base de dados com base nas informações fornecidas pelos utilizadores pertinentes nos termos do artigo 51.º, n.º 2. Os dados enumerados no anexo VIII-A são introduzidos na base de dados pelos fornecedores ou potenciais fornecedores, em conformidade com o artigo 54.º-A.

3. [suprimido]

4. A base de dados da UE não contém dados pessoais, exceto no que se refere às informações enumeradas no anexo VIII, e não prejudica o disposto no artigo 70.º.

5. A Comissão é considerada responsável pelo tratamento de dados da base de dados da UE. A Comissão disponibiliza aos fornecedores, potenciais fornecedores e utilizadores o apoio técnico e administrativo adequado.

5-A. As informações que constam da base de dados da UE registada em conformidade com o artigo 51.º devem estar acessíveis ao público. As informações registadas em conformidade com o artigo 54.º-A são acessíveis apenas às autoridades de fiscalização do mercado e à Comissão, a menos que o fornecedor ou potencial fornecedor tenha dado o seu consentimento para tornar essas informações igualmente acessíveis ao público.

TÍTULO VIII

ACOMPANHAMENTO PÓS-COMERCIALIZAÇÃO, PARTILHA DE INFORMAÇÕES, FISCALIZAÇÃO DO MERCADO

CAPÍTULO 1

ACOMPANHAMENTO PÓS-COMERCIALIZAÇÃO

Artigo 61.º

Acompanhamento pós-comercialização pelos fornecedores e plano de acompanhamento pós- comercialização aplicável a sistemas de inteligência artificial de risco elevado

1. Os fornecedores devem criar e documentar um sistema de acompanhamento pós-comercialização que seja proporcionado aos riscos do sistema de IA de risco elevado.

2. A fim de permitir ao fornecedor avaliar a conformidade dos sistemas de IA com os requisitos estabelecidos no título III, capítulo 2, ao longo do seu ciclo de vida, o sistema de acompanhamento pós-comercialização deve recolher, documentar e analisar dados pertinentes, que podem ser fornecidos pelos utilizadores ou podem ser recolhidos por meio de outras fontes sobre o desempenho dos sistemas de IA de risco elevado. Esta obrigação não abrange os dados operacionais sensíveis dos utilizadores de sistemas de IA que sejam autoridades policiais.

3. O sistema de monitorização pós-comercialização deve basear-se num plano de acompanhamento pós-comercialização. O plano de acompanhamento pós-comercialização deve fazer parte da documentação técnica referida no anexo IV. A Comissão adota um ato de execução com disposições pormenorizadas que estabeleçam um modelo para o plano de acompanhamento pós-comercialização e a lista de elementos a incluir no plano.

4. No respeitante aos sistemas de IA de risco elevado abrangidos pelos atos jurídicos referidos no anexo II, secção A, relativamente aos quais já se encontram estabelecidos um sistema e um plano de acompanhamento pós-comercialização ao abrigo dessa legislação, a documentação relativa ao acompanhamento pós-comercialização elaborada ao abrigo dessa legislação é considerada suficiente, desde que seja utilizado o modelo a que se refere o n.º 3.

O primeiro parágrafo também é aplicável aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, colocados no mercado ou colocados em serviço por instituições financeiras que estejam sujeitos a requisitos em matéria de governação, mecanismos ou processos internos ao abrigo da legislação da União no domínio dos serviços financeiros.

CAPÍTULO 2

PARTILHA DE INFORMAÇÕES SOBRE INCIDENTES GRAVES

Artigo 62.º

Comunicação de incidentes graves

1. Os fornecedores de sistemas de IA de risco elevado colocados no mercado da União devem comunicar quaisquer incidentes graves às autoridades de fiscalização do mercado dos Estados-Membros onde esse incidente ocorrer.

Essa notificação deve ser efetuada imediatamente após o fornecedor ter determinado uma relação causal entre o sistema de IA e o incidente grave ou a probabilidade razoável dessa relação e, em qualquer caso, o mais tardar 15 dias após o fornecedor ter conhecimento do incidente grave.

2. Após receção de uma notificação relacionada com um incidente grave a que se refere o artigo 3.º, n.º 44, alínea c), a autoridade de fiscalização do mercado relevante deve informar as autoridades ou os organismos públicos nacionais a que se refere o artigo 64.º, n.º 3. A Comissão elabora orientações específicas para facilitar o cumprimento das obrigações previstas no n.º 1. As referidas orientações devem ser publicadas, o mais tardar, 12 meses após a entrada em vigor do presente regulamento.

3. Relativamente aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, colocados no mercado ou colocados em serviço por fornecedores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos ao abrigo da legislação da União no domínio dos serviços financeiros, a notificação dos incidentes graves é limitada aos casos referidos no artigo 3.º, n.º 44, alínea c).

4. Relativamente aos sistemas de IA de risco elevado que sejam componentes de segurança de dispositivos ou sejam, eles próprios, dispositivos abrangidos pelos Regulamentos (UE) 2017/745 e (UE) 2017/746, a notificação de incidentes graves limita-se aos casos referidos no artigo 3.º, n.º 44, alínea c), e é feita à autoridade nacional competente escolhida para o efeito pelos Estados-Membros em que ocorreu o incidente.

CAPÍTULO 3

EXECUÇÃO

Artigo 63.º

Fiscalização do mercado e controlo dos sistemas de inteligência artificial presentes no mercado da União

1. O Regulamento (UE) 2019/1020 é aplicável aos sistemas de IA abrangidos pelo presente regulamento. Contudo, para efeitos da execução efetiva do presente regulamento:

   a) Qualquer referência a um operador económico nos termos do Regulamento (UE) 2019/1020 deve ser entendida como incluindo todos os operadores identificados no artigo 2.º do presente regulamento;

   b) Qualquer referência a um produto nos termos do Regulamento (UE) 2019/1020 deve ser entendida como incluindo todos os sistemas de IA que se enquadrem no âmbito do presente regulamento.

2. No âmbito das suas obrigações de comunicação nos termos do artigo 34.º, n.º 4, do Regulamento (UE) 2019/1020, as autoridades de fiscalização do mercado devem comunicar à Comissão os resultados das atividades de fiscalização do mercado pertinentes ao abrigo do presente regulamento.

3. No caso dos sistemas de IA de risco elevado relacionados com produtos aos quais se apliquem atos jurídicos enunciados no anexo II, secção A, a autoridade de fiscalização do mercado para efeitos do presente regulamento deve ser a autoridade responsável pelas atividades de fiscalização do mercado designada nos termos desses atos jurídicos ou, em circunstâncias justificadas e desde que a coordenação seja assegurada, outra autoridade pertinente identificada pelo Estado-Membro.

Os procedimentos a que se referem os artigos 65.º, 66.º, 67.º e 68.º do presente regulamento não se aplicam aos sistemas de IA relacionados com produtos aos quais se aplicam os atos jurídicos enumerados no anexo II, secção A, quando esses atos jurídicos já preveem procedimentos com o mesmo objetivo. Nesse caso, aplicam-se em vez disso os referidos procedimentos setoriais.

4. No caso dos sistemas de IA de risco elevado colocados no mercado, colocados em serviço ou utilizados por instituições financeiras regulamentadas pela legislação da União em matéria de serviços financeiros, a autoridade de fiscalização do mercado para efeitos do presente regulamento deve ser a autoridade nacional responsável pela supervisão financeira dessas instituições ao abrigo da referida legislação, na medida em que a colocação no mercado, a colocação em serviço ou a utilização do sistema de IA esteja diretamente relacionada com a prestação desses serviços financeiros.

Em derrogação do parágrafo anterior, em circunstâncias justificadas e desde que assegurada a coordenação, o Estado-Membro pode identificar outra autoridade pertinente como autoridade de fiscalização do mercado para efeitos do presente regulamento.

As autoridades nacionais de fiscalização do mercado que supervisionam as instituições de crédito regulamentadas pela Diretiva 2013/36/UE, que participam no Mecanismo Único de Supervisão (MUS) estabelecido pelo Regulamento (CE) n.º 1204/2013 do Conselho, deverão comunicar sem demora ao Banco Central Europeu todas as informações identificadas no âmbito das suas atividades de fiscalização do mercado que possam ser de interesse potencial para as atribuições de supervisão prudencial do Banco Central Europeu especificadas nesse regulamento.

5. No respeitante aos sistemas de IA de risco elevado enumerados no anexo III, ponto 1, alínea a), contanto que sejam utilizados para efeitos de manutenção da ordem pública, e pontos 6, 7 e 8, os Estados-Membros devem designar como autoridades de fiscalização do mercado para efeitos do presente regulamento as autoridades nacionais que fiscalizam as atividades das autoridades competentes em matéria de manutenção da ordem pública, controlo de fronteiras, imigração, asilo ou judiciária, ou as autoridades de controlo da proteção de dados competentes nos termos da Diretiva (UE) 2016/680 ou do Regulamento 2016/679. As atividades de fiscalização do mercado não devem, de modo algum, afetar a independência das autoridades judiciárias nem interferir com as suas atividades no exercício das suas funções judiciárias.

6. Sempre que as instituições, órgãos e organismos da União se insiram no âmbito do presente regulamento, a Autoridade Europeia para a Proteção de Dados deve atuar como a autoridade de fiscalização do mercado dos mesmos.

7. Os Estados-Membros devem facilitar a coordenação entre as autoridades de fiscalização do mercado designadas nos termos do presente regulamento e outras autoridades ou organismos nacionais competentes que supervisionam a aplicação da legislação de harmonização da União enunciada no anexo II ou de outra legislação da União que possa ser aplicável aos sistemas de IA de risco elevado referidos no anexo III.

8. Sem prejuízo dos poderes previstos no Regulamento (UE) 2019/1020, e sempre que pertinente e limitado ao necessário para o desempenho das suas funções, o fornecedor deve conceder às autoridades de fiscalização do mercado total acesso à documentação, bem como aos conjuntos de dados de treino, validação e teste utilizados para o desenvolvimento do sistema de IA de risco elevado, incluindo, se for caso disso e sob reserva de salvaguardas de segurança, através de interfaces de programação de aplicações ou outros meios e ferramentas técnicas pertinentes que possibilitem o acesso remoto.

9. Deve ser concedido às autoridades de fiscalização do mercado o acesso ao código-fonte do sistema de IA de risco elevado mediante pedido fundamentado e apenas se estiverem preenchidas cumulativamente as seguintes condições:

a) O acesso ao código-fonte é necessário para avaliar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no título III, capítulo 2, e

b) Os procedimentos de teste/auditoria e as verificações baseadas nos dados e na documentação apresentados pelo fornecedor foram esgotados ou revelaram-se insuficientes.

10. Todas as informações e documentação que as autoridades de fiscalização do mercado obtenham devem ser tratadas em conformidade com as obrigações de confidencialidade estabelecidas no artigo 70.º.

11. As queixas à autoridade de fiscalização do mercado pertinente podem ser apresentadas por qualquer pessoa singular ou coletiva que tenha motivos para considerar que houve uma infração às disposições do presente regulamento.

Em conformidade com o artigo 11.º, n.º 3, alínea e), e n.º 7, alínea a), do Regulamento (UE) 2019/1020, as queixas devem ser tidas em conta para efeitos da realização das atividades de fiscalização do mercado e tratadas em conformidade com os procedimentos específicos estabelecidos para o efeito pelas autoridades de fiscalização do mercado.

Artigo 63.º-A

Supervisão da testagem em condições reais pelas autoridades de fiscalização do mercado

1. As autoridades de fiscalização do mercado devem ter competência e poderes para assegurar que a testagem em condições reais está em conformidade com o presente regulamento.

2. Sempre que seja realizada uma testagem em condições reais para sistemas de IA supervisionados no âmbito de um ambiente de testagem da regulamentação da IA nos termos do artigo 54.º, as autoridades de fiscalização do mercado devem verificar a conformidade com as disposições do artigo 54.º-A no âmbito da sua função de supervisão do ambiente de testagem da regulamentação da IA. Essas autoridades podem, consoante o caso, permitir que a testagem em condições reais seja realizada pelo fornecedor ou potencial fornecedor em derrogação das condições estabelecidas no artigo 54.º-A, n.º 4, alíneas f) e g).

3. Se a autoridade de fiscalização do mercado for informada pelo fornecedor o potencial fornecedor ou por terceiros de um incidente grave ou tiver outros motivos para considerar que as condições estabelecidas nos artigos 54.º-A e 54.º-B não estão preenchidas, pode tomar qualquer uma das seguintes decisões no seu território, consoante o caso:

a) Suspender ou cessar a testagem em condições reais;

b) Solicitar ao fornecedor ou potencial fornecedor e ao(s) utilizador(es) que alterem qualquer aspeto da testagem em condições reais.

4. Se a autoridade de fiscalização do mercado tiver tomado uma das decisões referidas no n.º 3 do presente artigo ou emitido uma objeção na aceção do artigo 54.º-A, n.º 4, alínea b), a decisão ou objeção deve indicar os seus motivos e as modalidades e condições para o fornecedor ou potencial fornecedor contestar a decisão ou objeção.

5. Se for caso disso, sempre que uma autoridade de fiscalização do mercado tomar uma das decisões referidas no n.º 3 do presente artigo, deve comunicar os seus motivos às autoridades de fiscalização do mercado dos outros Estados-Membros em que o sistema de IA tenha sido testado em conformidade com o plano de testagem.

Artigo 64.º

Poderes das autoridades que protegem os direitos fundamentais

1. [suprimido]

2. [suprimido]

3. As autoridades ou organismos públicos nacionais que supervisionam ou asseguram, no atinente à utilização de sistemas de IA de risco elevado referidos no anexo III, o respeito das obrigações previstas na legislação da União que protege os direitos fundamentais, incluindo o direito à não discriminação, devem ter poderes para solicitar e aceder a toda a documentação elaborada ou mantida nos termos do presente regulamento, nos casos em que o acesso a essa documentação for necessário para o exercício das competências incluídas nos seus mandatos e dentro dos limites das respetivas jurisdições. A autoridade ou o organismo público competente deve informar a autoridade de fiscalização do mercado do Estado-Membro em causa de qualquer pedido dessa natureza.

4. No prazo de três meses a contar da entrada em vigor do presente regulamento, cada Estado-Membro deve identificar as autoridades ou os organismos públicos referidos no n.º 3 e tornar a lista acessível ao público. Os Estados-Membros devem notificar a lista à Comissão e a todos os outros Estados-Membros e mantê-la atualizada.

5. Se a documentação referida no n.º 3 for insuficiente para determinar se ocorreu um incumprimento de obrigações impostas por legislação da União destinada a proteger os direitos fundamentais, a autoridade ou o organismo público referido no n.º 3 pode apresentar um pedido fundamentado à autoridade de fiscalização do mercado para organizar a testagem do sistema de IA de risco elevado por recurso a meios técnicos. A autoridade de fiscalização do mercado deve organizar a testagem com a participação ativa da autoridade ou do organismo público requerente num prazo razoável após o pedido.

6. Todas as informações e documentação que as autoridades ou organismos públicos nacionais referidos no n.º 3 obtenham nos termos das disposições do presente artigo devem ser tratadas em conformidade com as obrigações de confidencialidade estabelecidas no artigo 70.º.

Artigo 65.º

Procedimento aplicável aos sistemas de inteligência artificial que apresentam riscos a nível nacional

1. Entende-se por "sistema de IA que apresenta um risco" um "produto que apresenta um risco", na aceção do artigo 3.º, ponto 19, do Regulamento (UE) 2019/1020, contanto que estejam em causa riscos para a saúde e a segurança ou para os direitos fundamentais das pessoas.

2. Se a autoridade de fiscalização do mercado de um Estado-Membro tiver motivos suficientes para considerar que um sistema de IA apresenta um risco, tal como descrito no n.º 1, deve avaliar o sistema de IA em causa no que diz respeito à conformidade do mesmo com todos os requisitos e obrigações previstos no presente regulamento. Se forem identificados riscos para os direitos fundamentais, a autoridade de fiscalização do mercado também deve informar as autoridades ou os organismos públicos nacionais competentes referidos no artigo 64.º, n.º 3. Os operadores envolvidos devem cooperar na medida do necessário com as autoridades de fiscalização do mercado e as outras autoridades ou organismos públicos nacionais referidos no artigo 64.º, n.º 3.

   Se, no decurso dessa avaliação, a autoridade de fiscalização do mercado verificar que o sistema de IA não cumpre os requisitos e as obrigações previstas no presente regulamento, deve exigir sem demora injustificada ao operador correspondente que tome todas as medidas corretivas adequadas para assegurar a conformidade do sistema de IA, para o retirar do mercado ou para o recolher num prazo fixado pela autoridade.

   A autoridade de fiscalização do mercado deve informar desse facto o organismo notificado pertinente. O artigo 18.º do Regulamento (UE) 2019/1020 é aplicável às medidas referidas no segundo parágrafo.

3. Se a autoridade de fiscalização do mercado considerar que a não conformidade não se limita ao respetivo território nacional, deve comunicar sem demora injustificada à Comissão e aos outros Estados-Membros os resultados da avaliação e as medidas que exigiu que o operador tomasse.

4. O operador deve garantir a aplicação de todas as medidas corretivas adequadas relativamente aos sistemas de IA em causa por si disponibilizados no mercado da União.

5. Se o operador de um sistema de IA não adotar as medidas corretivas adequadas no prazo referido no n.º 2, a autoridade de fiscalização do mercado deve tomar todas as medidas provisórias adequadas para proibir ou restringir a disponibilização do sistema de IA no respetivo mercado nacional, para o retirar do mercado ou para o recolher. A referida autoridade deve notificar sem demora injustificada a Comissão e os outros Estados-Membros da adoção de tais medidas.

6. A notificação referida no n.º 5 deve conter todas as informações disponíveis, em especial as informações necessárias à identificação do sistema de IA não conforme, a origem do sistema de IA, a natureza da alegada não conformidade e o risco conexo, a natureza e a duração das medidas nacionais adotadas, bem como as observações do operador em causa. As autoridades de fiscalização do mercado devem, nomeadamente, indicar se a não conformidade se deve a uma ou várias das seguintes razões:

-a) Incumprimento da proibição das práticas de inteligência artificial referidas no artigo 5.º;

a) O incumprimento, por parte do sistema de IA de risco elevado, dos requisitos estabelecidos no título III, capítulo 2;

b) Deficiências das normas harmonizadas ou das especificações comuns que, nos termos dos artigos 40.º e 41.º, conferem uma presunção de conformidade.

c) Incumprimento do disposto no artigo 52.º;

d) Incumprimento, por parte dos sistemas de IA de finalidade geral. dos requisitos e obrigações a que se refere o artigo 4.º-A;

7. As autoridades de fiscalização do mercado dos Estados-Membros, com exceção da autoridade de fiscalização do mercado do Estado-Membro que desencadeou o procedimento, devem informar sem demora injustificada a Comissão e os outros Estados-Membros das medidas tomadas e das informações adicionais de que disponham relativamente à não conformidade do sistema de IA em causa e, em caso de desacordo com a medida nacional notificada, das suas objeções.

8. Se, no prazo de três meses a contar da receção da notificação a que se refere o n.º 5, nem os Estados-Membros nem a Comissão tiverem levantado objeções à medida provisória tomada por um Estado-Membro, considera-se que a mesma é justificada. Esta disposição aplica-se sem prejuízo dos direitos processuais do operador em causa previstos no artigo 18.º do Regulamento (UE) 2019/1020. O prazo referido na primeira frase do presente número é reduzido para 30 dias em caso de incumprimento da proibição das práticas de inteligência artificial a que se refere o artigo 5.º.

9. As autoridades de fiscalização do mercado de todos os Estados-Membros devem então garantir que as medidas restritivas adequadas relativas ao sistema de IA em causa, bem como a retirada deste do respetivo mercado, sejam tomadas sem demora injustificada.

Artigo 66.º

Procedimento de salvaguarda da União

1. Se, nos três meses subsequentes à receção da notificação a que se refere o artigo 65.º, n.º 5, ou no prazo de 30 dias em caso de incumprimento da proibição das práticas de inteligência artificial a que se refere o artigo 5.º, um Estado-Membro levantar objeções a uma medida tomada por outro Estado-Membro, ou a Comissão considerar que a medida é contrária ao direito da União, a Comissão procede sem demora injustificada a consultas com a autoridade de fiscalização do mercado do Estado-Membro e o operador ou operadores em causa e avalia a medida nacional. Em função dos resultados dessa avaliação, a Comissão decide se a medida nacional é ou não justificada no prazo de nove meses, ou 60 dias em caso de incumprimento da proibição das práticas de inteligência artificial a que se refere o artigo 5.º, a contar da data da notificação a que se refere o artigo 65.º, n.º 5. A Comissão notifica essa decisão ao Estado-Membro em causa. A Comissão informa igualmente todos os outros Estados-Membros dessa decisão.

2. Se a medida tomada pela autoridade de fiscalização do mercado do Estado-Membro em causa for considerada justificada pela Comissão, as autoridades de fiscalização do mercado de todos os Estados-Membros devem garantir que são tomadas medidas restritivas adequadas relativamente ao sistema de IA em causa, como a retirada do sistema de IA do seu mercado sem demora injustificada, e devem informar a Comissão em conformidade. Se a medida nacional for considerada injustificada pela Comissão, a autoridade de fiscalização do mercado do Estado-Membro em causa retira a medida e informa a Comissão em conformidade.

3. Se a medida nacional for considerada justificada e a não conformidade do sistema de IA for atribuída a deficiências das normas harmonizadas ou das especificações comuns referidas nos artigos 40.º e 41.º do presente regulamento, a Comissão aplica o procedimento previsto no artigo 11.º do Regulamento (UE) n.º 1025/2012.

Artigo 67.º

Sistemas de inteligência artificial de risco elevado ou de finalidade geral conformes que apresentam um risco

1. Se, uma vez realizada a avaliação prevista no artigo 65.º, a autoridade de fiscalização do mercado de um Estado-Membro verificar que, embora conforme com o presente regulamento, um sistema de IA de risco elevado ou de finalidade geral apresenta um risco para a saúde ou a segurança das pessoas ou para os direitos fundamentais, deve exigir ao operador correspondente que tome todas as medidas adequadas para garantir que, quando o sistema de IA em causa for colocado no mercado ou colocado em serviço, já não apresenta esse risco, para retirar o sistema de IA do mercado ou para o recolher sem demora injustificada, num prazo que pode ser fixado pela autoridade.

2. O fornecedor ou outros operadores envolvidos devem assegurar que a medida corretiva seja tomada no tocante a todos os sistemas de IA em causa que tenham disponibilizado no mercado da União no prazo fixado pela autoridade de fiscalização do mercado do Estado-Membro referido no n.º 1.

3. O Estado-Membro deve informar imediatamente a Comissão e os restantes Estados-Membros deste facto. Essa notificação deve incluir todas as informações disponíveis, em particular os dados necessários à identificação do sistema de IA em causa, a origem e a cadeia de abastecimento do sistema de IA, a natureza do risco conexo e a natureza e duração das medidas nacionais adotadas.

4. A Comissão procede sem demora injustificada a consultas com os Estados-Membros em causa e com o operador em causa e avalia as medidas nacionais adotadas. Em função dos resultados dessa avaliação, a Comissão decide se a medida é ou não justificada e, se necessário, propõe medidas adequadas.

5. A Comissão designa os Estados-Membros em causa como destinatários da decisão e informa todos os outros Estados-Membros da mesma.

Artigo 68.º

Não conformidade formal

1. Se a autoridade de fiscalização do mercado de um Estado-Membro constatar um dos factos a seguir enunciados, deve exigir ao fornecedor em causa que ponha termo à não conformidade verificada, num prazo que pode ser fixado pela autoridade:

   a) A marcação de conformidade foi aposta em violação do disposto no artigo 49.º;

   b) A marcação de conformidade não foi aposta;

   c) A declaração de conformidade UE não foi elaborada;

   d) A declaração de conformidade UE não foi elaborada corretamente;

   e) O número de identificação do organismo notificado envolvido, se for caso disso, no procedimento de avaliação da conformidade não foi aposto.

2. Se a não conformidade referida no n.º 1 persistir, o Estado-Membro em causa deve tomar as medidas adequadas para restringir ou proibir a disponibilização no mercado do sistema de IA de risco elevado ou para garantir que o mesmo seja recolhido ou retirado do mercado.

Artigo 68.º-A

Instalações de ensaio da União no domínio da inteligência artificial

1. A Comissão designa uma ou mais instalações de ensaio da União nos termos do artigo 21.º do Regulamento (UE) 2019/1020 no domínio da inteligência artificial.

2. Sem prejuízo das atividades das instalações de ensaio da União a que se refere o artigo 21.º, n.º 6, do Regulamento (UE) 2019/1020, as instalações de ensaio da União a que se refere o n.º 1 devem também prestar aconselhamento técnico ou científico independente a pedido do Comité ou das autoridades de fiscalização do mercado.

Artigo 68.º-B

Grupo central de peritos independentes

1. A pedido do Comité para a Inteligência Artificial, a Comissão adota, por meio de um ato de execução, disposições sobre a criação, manutenção e financiamento de um grupo central de peritos independentes para apoiar as atividades de execução ao abrigo do presente regulamento.

2. Os peritos são selecionados pela Comissão e incluídos no grupo central com base em conhecimentos científicos ou técnicos atualizados no domínio da inteligência artificial, tendo devidamente em conta os domínios técnicos abrangidos pelos requisitos e obrigações previstos no presente regulamento e as atividades das autoridades de fiscalização do mercado nos termos do artigo 11.º do Regulamento (UE) 2019/1020. A Comissão determina o número de peritos no grupo em função das necessidades que se façam sentir.

3. Os peritos podem desempenhar as seguintes funções:

a) Aconselhar e apoiar o trabalho das autoridades de fiscalização do mercado, a pedido destas;

b) Apoiar as investigações de fiscalização do mercado transfronteiriças a que se refere o artigo 58.º, alínea h), sem prejuízo dos poderes das autoridades de fiscalização do mercado;

c) Aconselhar e apoiar a Comissão no exercício das suas funções no contexto da cláusula de salvaguarda nos termos do artigo 66.º.

4. Os peritos devem desempenhar as suas funções com imparcialidade e objetividade e garantir a confidencialidade das informações e dos dados obtidos no desempenho das suas funções e atividades. Cada um dos peritos apresenta uma declaração de interesses, que é disponibilizada ao público. A Comissão cria sistemas e procedimentos para gerir e evitar de forma ativa potenciais conflitos de interesses.

5. Os Estados-Membros podem ser obrigados a pagar honorários pelo aconselhamento e apoio prestados pelos peritos. A estrutura e o nível das honorários, bem como a escala e a estrutura das despesas reembolsáveis, são adotados pela Comissão por meio do ato de execução a que se refere o n.º 1, tendo em conta os objetivos de uma aplicação adequada do presente regulamento, a relação custo-eficácia e a necessidade de assegurar um acesso efetivo a peritos por parte de todos os Estados-Membros.

6. A Comissão facilita o acesso atempado dos Estados-Membros aos peritos, conforme necessário, e assegura que a combinação das atividades de apoio realizadas pelas instalações de ensaio da União nos termos do artigo 68.º-A e pelos peritos nos termos do presente artigo é organizada de forma eficiente e proporciona o melhor valor acrescentado possível.

TÍTULO IX

CÓDIGOS DE CONDUTA

Artigo 69.º

Códigos de conduta para a aplicação voluntária de requisitos específicos

1. A Comissão e os Estados-Membros facilitam a elaboração de códigos de conduta destinados a incentivar a aplicação voluntária de um ou mais dos requisitos estabelecidos no título III, capítulo 2, do presente regulamento a sistemas de IA que não sejam sistemas de IA de risco elevado, na medida do possível, tendo em conta as soluções técnicas disponíveis que permitam a aplicação desses requisitos.

2. A Comissão e o Comité facilitam a elaboração de códigos de conduta destinados a incentivar a aplicação voluntária a todos os sistemas de IA de requisitos específicos relacionados, por exemplo, com a sustentabilidade ambiental, nomeadamente no que diz respeito à programação eficiente em termos energéticos, à acessibilidade das pessoas com deficiência, à participação das partes interessadas na conceção e no desenvolvimento dos sistemas de IA e à diversidade das equipas de desenvolvimento, com base em objetivos claros e indicadores-chave de desempenho que permitam medir a consecução desses objetivos. A Comissão e os Estados-Membros facilitam igualmente, se adequado, a elaboração de códigos de conduta aplicáveis numa base voluntária no que diz respeito às obrigações dos utilizadores em relação aos sistemas de IA.

3. Os códigos de conduta aplicáveis numa base voluntária podem ser elaborados por fornecedores de sistemas de IA a título individual, por organizações que os representem, ou por ambos, nomeadamente com a participação de utilizadores e de quaisquer partes interessadas e das respetivas organizações representativas ou, se for caso disso, pelos utilizadores no que diz respeito às suas obrigações. Os códigos de conduta podem abranger um ou mais sistemas de IA, tendo em conta a semelhança da finalidade prevista desses sistemas.

4. A Comissão e os Estados-Membros devem ter em conta as necessidades e os interesses específicos dos fornecedores que são PME, inclusive as empresas em fase de arranque, quando incentivam e facilitam a elaboração de códigos de conduta a que se refere o presente artigo.

TÍTULO X

CONFIDENCIALIDADE E SANÇÕES

Artigo 70.º

Confidencialidade

1. As autoridades nacionais competentes, os organismos notificados, a Comissão, o Comité e qualquer outra pessoa singular ou coletiva envolvida na aplicação do presente regulamento adotam, nos termos da legislação da União ou nacional, medidas técnicas e organizativas adequadas para assegurar a confidencialidade das informações e dos dados obtidos no exercício das suas funções e atividades de modo a proteger, em especial:

a) Os direitos de propriedade intelectual e as informações comerciais confidenciais ou segredos comerciais de uma pessoa singular ou coletiva, incluindo o código-fonte, exceto nos casos a que se refere o artigo 5.º da Diretiva 2016/943 relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais;

b) A execução efetiva do presente regulamento, em especial no que diz respeito à realização de inspeções, investigações ou auditorias;

c) Os interesses públicos e nacionais em matéria de segurança;

d) A integridade de processos penais ou administrativos;

e) A integridade das informações classificadas nos termos da legislação da União ou nacional.

2. Sem prejuízo do n.º 1, no caso de sistemas de IA de risco elevado referidos no anexo III, pontos 1, 6 e 7, utilizados por autoridades competentes em matéria de manutenção da ordem pública, do controlo das fronteiras, de imigração ou de asilo, as informações trocadas numa base confidencial entre as autoridades nacionais competentes e entre as autoridades nacionais competentes e a Comissão não podem ser divulgadas sem consultar previamente a autoridade nacional competente de origem e o utilizador, quando tal divulgação prejudicar interesses públicos e nacionais em matéria de segurança. Esta obrigação de intercâmbio de informações não abrange dados operacionais sensíveis em relação às atividades das autoridades competentes em matéria de manutenção da ordem pública, de controlo de fronteiras, de imigração ou de asilo.

Se as autoridades competentes em matéria de manutenção da ordem pública, de imigração ou de asilo forem os fornecedores de sistemas de IA de risco elevado referidos no anexo III, pontos 1, 6 e 7, a documentação técnica referida no anexo IV deve permanecer nas instalações dessas autoridades. As referidas autoridades devem assegurar que as autoridades de fiscalização do mercado referidas no artigo 63.º, n.ºs 5 e 6, consoante o caso, possam, mediante pedido, aceder imediatamente à documentação ou obter uma cópia da mesma. O acesso à referida documentação ou a qualquer cópia da mesma só pode ser concedido ao pessoal da autoridade de fiscalização do mercado que detenha o nível apropriado de credenciação de segurança.

3. O disposto nos n.ºs 1 e 2 não afeta os direitos e obrigações da Comissão, dos Estados-Membros, das respetivas autoridades competentes e dos organismos notificados, no que se refere ao intercâmbio de informações e à divulgação de avisos, inclusive no contexto da cooperação transfronteiriça, nem o dever de informação que incumbe às partes em causa no âmbito do direito penal dos Estados-Membros.

Artigo 71.º

Sanções

1. Em conformidade com os termos e as condições previstas no presente regulamento, os Estados-Membros devem estabelecer o regime de sanções, incluindo coimas, aplicáveis em caso de infração ao presente regulamento e devem tomar todas as medidas necessárias para garantir que o mesmo é aplicado correta e eficazmente. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. Devem ter especialmente em conta a dimensão e os interesses dos fornecedores que são PME, incluindo as empresas em fase de arranque, e a respetiva viabilidade económica. Devem também ter em conta se a utilização do sistema de IA se insere no contexto de uma atividade pessoal de caráter não profissional.

2. Os Estados-Membros notificam a Comissão, sem demora, dessas regras e dessas medidas e também de qualquer alteração ulterior.

3. O incumprimento de qualquer uma das proibições das práticas de inteligência artificial a que se refere o artigo 5.º, fica sujeito a coimas até 30 000 000 EUR ou, se o infrator for uma empresa, até 6 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado. No caso das PME, incluindo as empresas em fase de arranque, estas coimas podem ir até 3 % do seu volume de negócios anual a nível mundial no exercício anterior.

4. Ficam sujeitas a coimas até 20 000 000 EUR ou, se o infrator for uma empresa, até 4 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado, as infrações às seguintes disposições relacionadas com operadores ou organismos notificados:

   -a) As obrigações dos fornecedores nos termos dos artigos 4.º-B e 4.º-C;

   a) As obrigações dos fornecedores nos termos dos artigo 16.º;

   b) As obrigações para determinadas outras pessoas nos termos do artigo 23.º-A;

c) As obrigações dos mandatários nos termos do artigo 25.º;

d) As obrigações dos importadores nos termos do artigo 26.º;

e) As obrigações dos distribuidores nos termos do artigo 27.º;

f) As obrigações dos utilizadores nos termos do artigo 29.º, n.ºs 1 a 6-A;

g) Os requisitos e obrigações dos organismos notificados nos termos do artigo 33.º, do artigo 34.º, n.ºs 1, 3 e 4, e do artigo 34.º-A;

h) As obrigações de transparência para os fornecedores e utilizadores nos termos do artigo 52.º.

No caso das PME, incluindo as empresas em fase de arranque, estas coimas podem ir até 2 % do seu volume de negócios anual a nível mundial no exercício financeiro anterior.

5. O fornecimento de informações incorretas, incompletas ou enganadoras aos organismos notificados e às autoridades nacionais competentes em resposta a um pedido fica sujeito a coimas até 10 000 000 EUR ou, se o infrator for uma empresa, até 2 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado. No caso das PME, incluindo as empresas em fase de arranque, estas coimas podem ir até 1 % do seu volume de negócios anual a nível mundial no exercício financeiro anterior.

6. A decisão relativa ao montante da coima a aplicar em cada caso deve ter em conta todas as circunstâncias pertinentes da situação específica, bem como os seguintes elementos:

a) A natureza, a gravidade e a duração da infração e das suas consequências;

a-A) O caráter intencional ou negligente da infração;

a-B) As medidas tomadas pelo operador para sanar a infração e atenuar os seus eventuais efeitos negativos;

b) O facto de outras autoridades de fiscalização do mercado noutros Estados-Membros já terem ou não aplicado coimas ao mesmo operador pela mesma infração;

b-A) O facto de outras autoridades já terem ou não aplicado coimas ao mesmo operador por infrações a outra legislação da União ou nacional, quando tais infrações resultarem da mesma atividade ou omissão que constitua uma infração pertinente ao presente ato legislativo;

c) A dimensão, o volume de negócios anual e a quota-parte de mercado do operador que cometeu a infração;

d) Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração.

7. Cada Estado-Membro deve definir regras que permitam determinar se e em que medida podem ser aplicadas coimas às autoridades e organismos públicos estabelecidos nesse Estado-Membro.

8. Dependendo do ordenamento jurídico dos Estados-Membros, as regras relativas às coimas podem ser aplicadas de maneira que as coimas sejam impostas por tribunais nacionais ou por outros organismos competentes, tal como previsto nesses Estados-Membros.
A aplicação dessas regras nesses Estados-Membros deve ter um efeito equivalente.

9. O exercício, por parte da autoridade de fiscalização do mercado, das competências que lhe são atribuídas pelo presente artigo fica sujeito às garantias processuais adequadas nos termos do direito da União e dos Estados-Membros, incluindo o direito à ação judicial e a um processo equitativo.

Artigo 72.º

Coimas aplicáveis às instituições, órgãos e organismos da União

1. A Autoridade Europeia para a Proteção de Dados pode impor coimas às instituições, órgãos e organismos da União que se enquadrem no âmbito do presente regulamento. Ao decidir sobre a imposição de uma coima e o montante da mesma, devem ser tidas em conta, em cada caso, todas as circunstâncias pertinentes da situação específica, bem como os seguintes elementos:

   a) A natureza, a gravidade e a duração da infração e das suas consequências;

   b) A cooperação com a Autoridade Europeia para a Proteção de Dados no sentido de corrigir a infração e atenuar os possíveis efeitos adversos da mesma, nomeadamente o cumprimento de eventuais medidas previamente impostas pela Autoridade Europeia para a Proteção de Dados contra a instituição, órgão ou organismo da União em causa relativamente à mesma matéria;

   c) Quaisquer infrações similares anteriormente cometidas pela instituição, órgão ou organismo da União.

2. O incumprimento de qualquer das proibições das práticas de inteligência artificial a que se refere o artigo 5.º fica sujeito a coimas até 500 000 EUR.

3. A não conformidade do sistema de IA com quaisquer requisitos ou obrigações por força do presente regulamento, que não os estabelecidos nos artigos 5.º e 10.º, fica sujeita a coimas até 250 000 EUR.

4. Antes de tomar decisões nos termos do presente artigo, a Autoridade Europeia para a Proteção de Dados deve conceder à instituição, órgão ou organismo da União objeto do procedimento por si aplicado a oportunidade de se pronunciar sobre a matéria que constitui possível infração. A Autoridade Europeia para a Proteção de Dados deve basear as suas decisões unicamente nos elementos e nas circunstâncias relativamente às quais as partes em causa puderam apresentar as observações. Os queixosos, caso existam, devem ser estreitamente associados ao procedimento.

5. Os direitos de defesa das partes em causa devem ser plenamente respeitados no desenrolar do processo. As partes interessadas devem ter o direito de aceder ao processo da Autoridade Europeia para a Proteção de Dados, sob reserva do interesse legítimo dos indivíduos ou das empresas relativamente à proteção dos respetivos dados pessoais ou segredos comerciais.

6. Os fundos recolhidos em resultado da imposição das coimas previstas no presente artigo constituem receitas do orçamento geral da União.

TÍTULO XI

DELEGAÇÃO DE PODERES E PROCEDIMENTO DE COMITÉ

Artigo 73.º

Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 7.º, n.ºs 1 e 3, no artigo 11.º, n.º 3, no artigo 43.º, n.ºs 5 e 6, e no artigo 48.º, n.º 5, é conferido à Comissão por um período de cinco anos a contar de [*data de entrada em vigor do presente regulamento*].

A Comissão elabora um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada prazo.

3. A delegação de poderes referida no artigo 7.º, n.º 1, no artigo 7.º, n.º 3, no artigo 11.º, n.º 3, no artigo 43.º, n.ºs 5 e 6, e no artigo 48.º, n.º 5, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou numa data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

5. Os atos delegados adotados nos termos do artigo 7.º, n.º 1, do artigo 7.º, n.º 3, do artigo 11.º, n.º 3, do artigo 43.º, n.ºs 5 e 6, e do artigo 48.º, n.º 5, só entram em vigor se nem o Parlamento Europeu nem o Conselho formularem objeções no prazo de três meses a contar da notificação desses atos a estas duas instituições ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não formularão objeções. O referido prazo é prorrogável por três meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 74.º

Procedimento de comité

1. A Comissão é assistida por um comité. Este comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

TÍTULO XII

DISPOSIÇÕES FINAIS

Artigo 75.º

Alteração do Regulamento (CE) n.º 300/2008

Ao artigo 4.º, n.º 3, do Regulamento (CE) n.º 300/2008, é aditado o seguinte parágrafo:

"Aquando da adoção de medidas de execução relacionadas com especificações técnicas e procedimentos para a aprovação e utilização de equipamentos de segurança respeitantes a sistemas de inteligência artificial na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).";

Artigo 76.º

Alteração do Regulamento (UE) n.º 167/2013

Ao artigo 17.º, n.º 5, do Regulamento (UE) n.º 167/2013, é aditado o seguinte parágrafo:

"Aquando da adoção de atos delegados nos termos do primeiro parágrafo relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).";

Artigo 77.º

Alteração do Regulamento (UE) n.º 168/2013

Ao artigo 22.º, n.º 5, do Regulamento (UE) n.º 168/2013, é aditado o seguinte parágrafo:

"Aquando da adoção de atos delegados nos termos do primeiro parágrafo relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).";

Artigo 78.º

Alteração da Diretiva 2014/90/UE

Ao artigo 8.º da Diretiva 2014/90/UE, é aditado o seguinte número:

"4. Aquando da realização das suas atividades nos termos do n.º 1 e da adoção de especificações técnicas e normas de ensaio em conformidade com os n.ºs 2 e 3 respeitantes a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, Comissão tem em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).".

Artigo 79.º

Alteração da Diretiva (UE) 2016/797

Ao artigo 5.º da Diretiva (UE) 2016/797, é aditado o seguinte número:

"12. Aquando da adoção de atos delegados nos termos do n.º 1 e de atos de execução nos termos do n.º 11 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).".

Artigo 80.º

Alteração do Regulamento (UE) 2018/858

Ao artigo 5.º do Regulamento (UE) 2018/858, é aditado o seguinte número:

"4. Aquando da adoção de atos delegados nos termos do n.º 3 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).".

Artigo 81.º

Alteração do Regulamento (UE) 2018/1139

O Regulamento (UE) 2018/1139 é alterado do seguinte modo:

1) Ao artigo 17.º, é aditado o seguinte número:

"3. Sem prejuízo do disposto no n.º 2, aquando da adoção de atos de execução nos termos do n.º 1 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [*relativo à inteligência artificial*]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).";

2) Ao artigo 19.º, é aditado o seguinte número:

"4. Aquando da adoção de atos delegados nos termos dos n.ºs 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.";

3) Ao artigo 43.º, é aditado o seguinte número:

"4. Aquando da adoção de atos de execução nos termos do n.º 1 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.";

4) Ao artigo 47.º, é aditado o seguinte número:

"3. Aquando da adoção de atos delegados nos termos dos n.ºs 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.";

5) Ao artigo 57.º, é aditado o seguinte número:

"Aquando da adoção desses atos de execução relativamente a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.".

6) Ao artigo 58.º, é aditado o seguinte número:

"3. Aquando da adoção de atos delegados nos termos dos n.ºs 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.".

Artigo 82.º

Alteração do Regulamento (UE) 2019/2144

Ao artigo 11.º do Regulamento (UE) 2019/2144, é aditado o seguinte número:

"3. Aquando da adoção de atos de execução nos termos do n.º 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).".

Artigo 83.º

Sistemas de inteligência artificial já colocados no mercado ou em serviço

1. O presente regulamento não se aplica aos sistemas de IA que sejam componentes de sistemas informáticos de grande escala criados pelos atos jurídicos enumerados no anexo IX que tenham sido colocados no mercado ou colocados em serviço antes de *[12 meses após a data de aplicação do presente regulamento referida no artigo 85.º, n.º 2]*, salvo se a substituição ou alteração desses atos jurídicos implicar uma alteração significativa da conceção ou da finalidade prevista do sistema ou dos sistemas de IA em causa.

   Os requisitos estabelecidos no presente regulamento devem ser tidos em conta, se for caso disso, na avaliação de cada um dos sistemas informáticos de grande escala criados pelos atos jurídicos enumerados no anexo IX, a realizar como previsto nos respetivos atos.

2. O presente regulamento só se aplica aos sistemas de IA de risco elevado, que não os referidos no n.º 1, que tenham sido colocados no mercado ou colocados em serviço antes de [*data de aplicação do presente regulamento referida no artigo 85.º, n.º 2*], se, após essa data, os referidos sistemas forem sujeitos a alterações significativas em termos de conceção ou finalidade prevista.

Artigo 84.º

Avaliação e reexame

1. [suprimido]

1-B. A Comissão avalia a necessidade de alterar a lista que consta do anexo III a cada 24 meses após a entrada em vigor do presente regulamento e até ao final do período de delegação de poderes. As conclusões dessa avaliação são apresentadas ao Parlamento Europeu e ao Conselho.

2. Até [*três anos após a data de aplicação do presente regulamento referida no artigo 85.º, n.º 2*] e subsequentemente de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e reexame do presente regulamento. Os relatórios devem ser divulgados ao público.

3. Os relatórios referidos no n.º 2 devem dar especial atenção ao seguinte:

   a) A situação das autoridades nacionais competentes em termos de recursos financeiros, equipamento técnico e recursos humanos necessários para exercer eficazmente as funções que lhes foram atribuídas nos termos do presente regulamento;

   b) O estado das sanções, designadamente das coimas referidas no artigo 71.º, n.º 1, aplicadas pelos Estados-Membros em consequência de infrações às disposições do presente regulamento.

4. No prazo de [*três anos a contar da data de aplicação do presente regulamento referida no artigo 85.º, n.º 2*] e subsequentemente de quatro em quatro anos, se adequado, a Comissão avalia o impacto e a eficácia dos códigos de conduta voluntários com vista a fomentar a aplicação dos requisitos estabelecidos no título III, capítulo 2, a sistemas de IA que não sejam sistemas de IA de risco elevado e, eventualmente, de outros requisitos adicionais a sistemas de IA, incluindo no que diz respeito à sustentabilidade ambiental.

5. Para efeitos do disposto nos n.ºs 1-A a 4, o Comité, os Estados-Membros e as autoridades nacionais competentes devem facultar à Comissão as informações que esta solicitar.

6. Ao efetuar as avaliações e os reexames a que se referem os n.ºs 1-A a 4, a Comissão tem em consideração as posições e as conclusões do Comité, do Parlamento Europeu, do Conselho e de outros organismos ou fontes pertinentes.

7. Se necessário, a Comissão apresenta propostas adequadas com vista a alterar o presente regulamento, atendendo, em especial, à evolução das tecnologias e aos progressos da sociedade da informação.

Artigo 85.º

Entrada em vigor e aplicação

1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

2. O presente regulamento é aplicável a partir de [36 meses após a sua entrada em vigor].

3. Em derrogação do disposto no n.º 2:

   a) O título III, capítulo 4, e o título VI são aplicáveis a partir de [12 meses após a entrada em vigor do presente regulamento];

   b) O artigo 71.º é aplicável a partir de [12 meses após a entrada em vigor do presente regulamento].

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente/A Presidente	*O Presidente/A Presidente*

ANEXO I

[suprimido]

ANEXO II

LISTA DA LEGISLAÇÃO DE HARMONIZAÇÃO DA UNIÃO

Secção A – Lista da legislação de harmonização da União baseada no novo quadro legislativo

1. Diretiva 2006/42/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006, relativa às máquinas e que altera a Diretiva 95/16/CE (JO L 157 de 9.6.2006, p. 24) [revogada pelo Regulamento Máquinas];

2. Diretiva 2009/48/CE do Parlamento Europeu e do Conselho, de 18 de junho de 2009, relativa à segurança dos brinquedos (JO L 170 de 30.6.2009, p. 1);

3. Diretiva 2013/53/UE do Parlamento Europeu e do Conselho, de 20 de novembro de 2013, relativa às embarcações de recreio e às motas de água e que revoga a Diretiva 94/25/CE (JO L 354 de 28.12.2013, p. 90);

4. Diretiva 2014/33/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante a ascensores e componentes de segurança para ascensores (JO L 96 de 29.3.2014, p. 251);

5. Diretiva 2014/34/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização da legislação dos Estados-Membros relativa a aparelhos e sistemas de proteção destinados a ser utilizados em atmosferas potencialmente explosivas (JO L 96 de 29.3.2014, p. 309);

6. Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado e que revoga a Diretiva 1999/5/CE (JO L 153 de 22.5.2014, p. 62);

7. Diretiva 2014/68/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos sob pressão no mercado (JO L 189 de 27.6.2014, p. 164);

8. Regulamento (UE) 2016/424 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo às instalações por cabo e que revoga a Diretiva 2000/9/CE (JO L 81 de 31.3.2016, p. 1);

9. Regulamento (UE) 2016/425 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo aos equipamentos de proteção individual e que revoga a Diretiva 89/686/CEE do Conselho (JO L 81 de 31.3.2016, p. 51);

10. Regulamento (UE) 2016/426 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo aos aparelhos a gás e que revoga a Diretiva 2009/142/CE do Conselho (JO L 81 de 31.3.2016, p. 99);

11. Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho (JO L 117 de 5.5.2017, p. 1);

12. Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos para diagnóstico in vitro e que revoga a Diretiva 98/79/CE e a Decisão 2010/227/UE da Comissão (JO L 117 de 5.5.2017, p. 176).

Secção B – Lista de outra legislação de harmonização da União

1. Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).

2. Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação e fiscalização do mercado dos veículos de duas ou três rodas e dos quadriciclos (JO L 60 de 2.3.2013, p. 52);

3. Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho, de 5 de fevereiro de 2013, relativo à homologação e fiscalização do mercado de tratores agrícolas e florestais (JO L 60 de 2.3.2013, p. 1);

4. Diretiva 2014/90/UE do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativa aos equipamentos marítimos e que revoga a Diretiva 96/98/CE do Conselho (JO L 257 de 28.8.2014, p. 146);

5. Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, relativa à interoperabilidade do sistema ferroviário na União Europeia (JO L 138 de 26.5.2016, p. 44).

6. Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativo à homologação e à fiscalização do mercado dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a esses veículos, que altera os Regulamentos (CE) n.º 715/2007 e (CE) n.º 595/2009 e revoga a Diretiva 2007/46/CE (JO L 151 de 14.6.2018, p. 1);

7. Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativo aos requisitos de homologação de veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos, no que se refere à sua segurança geral e à proteção dos ocupantes dos veículos e dos utentes da estrada vulneráveis, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 78/2009, (CE) n.º 79/2009 e (CE) n.º 661/2009 do Parlamento Europeu e do Conselho e os Regulamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012, e (UE) n.º 2015/166 da Comissão (JO L 325 de 16.12.2019, p. 1);

8. Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, de 4 de julho de 2018, relativo a regras comuns no domínio da aviação civil que cria a Agência da União Europeia para a Segurança da Aviação, altera os Regulamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010 e (UE) n.º 376/2014 e as Diretivas 2014/30/UE e 2014/53/UE do Parlamento Europeu e do Conselho, e revoga os Regulamentos (CE) n.º 552/2004 e (CE) n.º 216/2008 do Parlamento Europeu e do Conselho e o Regulamento (CEE) n.º 3922/91 do Conselho (JO L 212 de 22.8.2018, p. 1), no que se refere ao projeto, fabrico e colocação no mercado de aeronaves a que se refere o artigo 2.º, n.º 1, alíneas a) e b), na parte relativa a aeronaves não tripuladas e aos seus motores, hélices, peças e equipamento de controlo remoto.

ANEXO III

SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO A QUE SE REFERE O ARTIGO 6.º, N.º 3

Em cada um dos domínios enumerados nos pontos 1-8, os sistemas de IA especificamente mencionados em cada alínea são considerados sistemas de IA de risco elevado nos termos do artigo 6.º, n.º 3:

1. Biometria:

   a) Sistemas de identificação biométrica à distância.

2. Infraestruturas críticas:

   (a) Sistemas de IA concebidos para serem utilizados como componentes de segurança na gestão e no controlo de infraestruturas digitais críticas, do trânsito rodoviário e das redes de abastecimento de água, gás, aquecimento e eletricidade.

3. Educação e formação profissional:

   (a) Sistemas de IA concebidos para serem utilizados para determinar o acesso, a admissão ou a afetação de pessoas singulares a instituições de ensino e de formação profissional ou a programas de todos os níveis;

   (b) Sistemas de IA concebidos para serem utilizados para avaliar os resultados da aprendizagem, nomeadamente quando esses resultados são utilizados para orientar o processo de aprendizagem de pessoas singulares em instituições de ensino e de formação profissional ou em programas de todos os níveis.

4. Emprego, gestão de trabalhadores e acesso ao emprego por conta própria:

   (a) Sistemas de IA concebidos para serem utilizados no recrutamento ou na seleção de pessoas singulares, designadamente para colocar anúncios de emprego direcionados, analisar e filtrar candidaturas a ofertas de emprego e avaliar os candidatos;

(b) Sistemas de IA concebidos para serem utilizados na tomada de decisões sobre promoções ou cessações de relações contratuais de trabalho, sobre a repartição de tarefas com base em comportamentos individuais ou traços ou características de personalidade e sobre o controlo e avaliação do desempenho e do comportamento de pessoas envolvidas nas referidas relações.

5. Acesso a serviços privados essenciais e a serviços e prestações públicas essenciais, bem como o usufruto dos mesmos:

(a) Sistemas de IA concebidos para serem utilizados por autoridades públicas ou em nome de autoridades públicas para avaliar a elegibilidade de pessoas singulares quanto a prestações e serviços públicos essenciais de assistência, bem como para conceder, reduzir, revogar ou recuperar tais prestações e serviços;

(b) Sistemas de IA concebidos para serem utilizados para avaliar a capacidade de endividamento de pessoas singulares ou estabelecer a sua classificação de crédito, com exceção dos sistemas de IA colocados em serviço por fornecedores que são micro e pequenas empresas, conforme definidas no anexo da Recomendação da Comissão 2003/361/CE, para utilização própria;

(c) Sistemas de IA concebidos para serem utilizados no envio ou no estabelecimento de prioridades no envio de serviços de resposta a emergências, incluindo bombeiros e assistência médica;

(d) Sistemas de IA concebidos para serem utilizados nas avaliações de risco e na fixação de preços em relação a pessoas singulares, com exceção dos sistemas de IA colocados em serviço por fornecedores que são micro e pequenas empresas, conforme definidas no anexo da Recomendação da Comissão 2003/361/CE, para utilização própria;

6. Manutenção da ordem pública:

(a) Sistemas de IA concebidos para serem utilizados por autoridades policiais, ou em seu nome, a fim de determinar o risco de uma pessoa singular cometer infrações ou voltar a cometer infrações ou o risco de uma pessoa singular se tornar uma potencial vítima de infrações penais;

(b) Sistemas de IA concebidos para serem utilizados por autoridades policiais, ou em seu nome, como polígrafos e instrumentos similares ou para detetar o estado emocional de uma pessoa singular;

(c) [suprimido]

(d) Sistemas de IA concebidos para serem utilizados por autoridades policiais, ou em seu nome, para avaliar a fiabilidade dos elementos de prova no decurso da investigação ou repressão de infrações penais;

(e) Sistemas de IA concebidos para serem utilizados por autoridades policiais, ou em seu nome, para prever a ocorrência ou a recorrência de uma infração penal real ou potencial com base na definição de perfis de pessoas singulares, na aceção do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680, ou para avaliar os traços de personalidade e as características ou os comportamento criminal passado de pessoas singulares ou grupos;

(f) Sistemas de IA concebidos para serem utilizados por autoridades policiais, ou em seu nome, para definir o perfil de pessoas singulares, na aceção do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680, no decurso da deteção, investigação ou repressão de infrações penais;

(g) [suprimido]

7. Gestão da migração, do asilo e do controlo das fronteiras:

(a) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes, ou em seu nome, como polígrafos e instrumentos similares ou para detetar o estado emocional de uma pessoa singular;

(b) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes, ou em seu nome, para avaliar riscos, incluindo um risco para a segurança, um risco de migração irregular ou um risco para a saúde, representados por uma pessoa singular que pretenda entrar ou tenha entrado no território de um Estado-Membro;

(c) [suprimido]

(d) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes, ou em seu nome, na análise dos pedidos de asilo, de visto e de autorização de residência e das queixas relacionadas, no que toca à elegibilidade das pessoas singulares que requerem determinado estatuto.

8. Administração da justiça e processos democráticos:

(a) Sistemas de IA concebidos para serem utilizados por uma autoridade judiciária, ou em seu nome, na interpretação de factos ou do direito e na aplicação da lei a um conjunto específico de factos.

ANEXO IV

DOCUMENTAÇÃO TÉCNICA referida no artigo 11.º, n.º 1

A documentação técnica referida no artigo 11.º, n.º 1, deve conter, pelo menos, as informações indicadas a seguir, consoante aplicável ao sistema de IA em causa:

1. Uma descrição geral do sistema de IA, nomeadamente:

   (a) A finalidade prevista, a(s) pessoa(s) responsáveis pelo seu desenvolvimento, a data e a versão do sistema;

   (b) De que forma o sistema de IA interage ou pode ser utilizado para interagir com hardware ou software que não faça parte do próprio sistema de IA, se for caso disso;

   (c) As versões do software ou firmware instalado e quaisquer requisitos relacionados com a atualização das versões;

   (d) A descrição de todas as formas sob as quais o sistema de IA é colocado no mercado ou colocado em serviço (por exemplo, em forma de pacote de software integrado em hardware, em formato descarregável, através de interfaces de programação de aplicações, entre outros);

   (e) A descrição do hardware no qual se pretende executar o sistema de IA;

   (f) Se o sistema de IA for um componente de produtos, fotografias ou ilustrações que revelem as características externas, a marcação e a disposição interna desses produtos;

   (g) Instruções de utilização para o utilizador e, se for caso disso, instruções de instalação;

2. Uma descrição pormenorizada dos elementos do sistema de IA e do respetivo processo de desenvolvimento, incluindo:

   (a) Os métodos utilizados e os passos dados com vista ao desenvolvimento do sistema de IA, incluindo, se for caso disso, o recurso a sistemas ou ferramentas previamente treinados fornecidos por terceiros e de que forma estes foram utilizados, integrados ou modificados pelo fornecedor;

(b) As especificações de conceção do sistema, designadamente a lógica geral do sistema de IA e dos algoritmos; as principais opções de conceção, nomeadamente a lógica subjacente e os pressupostos utilizados, também no respeitante às pessoas ou grupos de pessoas em relação às quais se pretende que o sistema seja utilizado; as principais opções de classificação; o que se pretende otimizar com o sistema e a importância dos diferentes parâmetros; a descrição dos resultados esperados do sistema; as decisões acerca de eventuais cedências em relação às soluções técnicas adotadas para cumprir os requisitos definidos no título III, capitulo 2;

(c) A descrição da arquitetura do sistema, explicando de que forma os componentes de software se incorporam ou enriquecem mutuamente e como se integram no processamento global; os recursos computacionais utilizados para desenvolver, treinar, testar e validar o sistema de IA;

(d) Se for caso disso, os requisitos de dados em termos de folhas de dados que descrevam as metodologias e técnicas de treino e os conjuntos de dados de treino utilizados, incluindo uma descrição geral desses conjuntos de dados, informações sobre a sua proveniência, o seu âmbito e as suas principais características; de que forma os dados foram obtidos e selecionados; procedimentos de rotulagem (por exemplo, para aprendizagem supervisionada), metodologias de limpeza de dados (por exemplo, deteção de valores atípicos);

(e) Análise das medidas de supervisão humana necessárias em conformidade com o artigo 14.º, incluindo uma análise das soluções técnicas necessárias para facilitar a interpretação dos resultados dos sistemas de IA pelos utilizadores, em conformidade com o artigo 13.º, n.º 3, alínea d);

(f) Se for caso disso, uma descrição pormenorizada das alterações predeterminadas do sistema de IA e do seu desempenho, juntamente com todas as informações pertinentes relacionadas com as soluções técnicas adotadas para assegurar a conformidade contínua do sistema de IA com os requisitos aplicáveis estabelecidos no título III, capítulo 2;

(g) Os procedimentos de validação e testagem aplicados, incluindo informações sobre os dados de validação e testagem utilizados e as principais características desses dados; as métricas utilizadas para aferir a exatidão, a solidez, a cibersegurança e a conformidade com outros requisitos aplicáveis estabelecidos no título III, capítulo 2, bem como potenciais impactos discriminatórios; registos dos testes e todos os relatórios de teste datados e assinados pelas pessoas responsáveis, incluindo no respeitante às alterações predeterminadas referidas na alínea f).

3. Informações pormenorizadas sobre o acompanhamento, o funcionamento e o controlo do sistema de IA, especialmente no que diz respeito: às suas capacidades e limitações de desempenho, incluindo os níveis de exatidão no tocante a pessoas ou grupos de pessoas específicos em relação às quais se pretende que o sistema seja utilizado e o nível geral esperado de exatidão em relação à finalidade prevista; os resultados não pretendidos mas previsíveis e as fontes de riscos para a saúde e a segurança, os direitos fundamentais e a proteção contra a discriminação atendendo à finalidade prevista do sistema de IA; as medidas de supervisão humana necessárias em conformidade com o artigo 14.º, incluindo as soluções técnicas adotadas para facilitar a interpretação dos resultados dos sistemas de IA pelos utilizadores; especificações relativas aos dados de entrada, consoante apropriado;

4. Uma descrição pormenorizada do sistema de gestão de riscos em conformidade com o artigo 9.º;

5. A descrição das alterações pertinentes introduzidas no sistema pelo fornecedor ao longo do seu ciclo de vida;

6. Uma lista de normas harmonizadas aplicadas total ou parcialmente, cujas referências tenham sido publicadas no Jornal Oficial da União Europeia; caso não tenham sido aplicadas tais normas harmonizadas, uma descrição pormenorizada das soluções adotadas para cumprir os requisitos estabelecidos no título III, capítulo 2, incluindo uma lista de outras normas pertinentes e especificações técnicas aplicadas;

7. Uma cópia da declaração de conformidade UE;

8. Uma descrição pormenorizada do sistema existente para avaliar o desempenho do sistema de IA na fase de pós-comercialização em conformidade com o artigo 61.º, nomeadamente o plano de acompanhamento pós-comercialização referido no artigo 61.º, n.º 3.

ANEXO V
DECLARAÇÃO DE CONFORMIDADE UE

A declaração de conformidade UE referida no artigo 48.º deve conter todas as seguintes informações:

1. Nome e tipo do sistema de IA e quaisquer outras referências inequívocas que permitam identificar e rastrear o sistema de IA;

2. Nome e endereço do fornecedor ou, se aplicável, do mandatário;

3. Menção de que a declaração de conformidade UE é emitida sob a exclusiva responsabilidade do fornecedor;

4. Menção que ateste que o sistema de IA em causa é conforme com o presente regulamento e, se for caso disso, com outra legislação da União aplicável que preveja a emissão de declarações de conformidade UE;

5. Referências a quaisquer normas harmonizadas aplicáveis utilizadas ou a quaisquer outras especificações comuns em relação às quais é declarada a conformidade;

6. Se for caso disso, nome e número de identificação do organismo notificado, descrição do procedimento de avaliação da conformidade adotado e identificação do certificado emitido;

7. Local e data de emissão da declaração, nome e cargo da pessoa que assina, bem como indicação da pessoa em nome de quem assina, assinatura.

ANEXO VI

PROCEDIMENTO DE AVALIAÇÃO DA CONFORMIDADE BASEADO NO CONTROLO INTERNO

1. O procedimento de avaliação da conformidade baseado no controlo interno é o descrito nos pontos 2 a 4.

2. O fornecedor verifica se o sistema de gestão da qualidade aplicado se encontra em conformidade com os requisitos do artigo 17.º.

3. O fornecedor analisa as informações contidas na documentação técnica para determinar a conformidade do sistema de IA com os requisitos essenciais aplicáveis estabelecidos no título III, capítulo 2.

4. O fornecedor também verifica se o processo de conceção e desenvolvimento do sistema de IA e do seu acompanhamento pós-comercialização referido no artigo 61.º estão de acordo com a documentação técnica.

ANEXO VII

CONFORMIDADE BASEADA NA AVALIAÇÃO DO SISTEMA DE GESTÃO DA QUALIDADE E NA AVALIAÇÃO DA DOCUMENTAÇÃO TÉCNICA

1. Introdução

A conformidade baseada na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica é o procedimento de avaliação da conformidade descrito nos pontos 2 a 5.

2. Visão geral

O sistema de gestão da qualidade aprovado para efeitos de conceção, desenvolvimento e testagem de sistemas de IA nos termos do artigo 17.º é analisado em conformidade com o ponto 3 e está sujeito à fiscalização especificada no ponto 5. A documentação técnica do sistema de IA é analisada em conformidade com o ponto 4.

3. Sistema de gestão da qualidade

3.1. O pedido do fornecedor inclui:

(a) O nome e o endereço do fornecedor e, se for apresentado pelo mandatário, o nome e o endereço deste último;

(b) A lista dos sistemas de IA abrangidos pelo mesmo sistema de gestão da qualidade;

(c) A documentação técnica de cada sistema de IA abrangido pelo mesmo sistema de gestão da qualidade;

(d) A documentação relativa ao sistema de gestão da qualidade, que abrange todos os aspetos enunciados no artigo 17.º;

(e) Uma descrição dos procedimentos em vigor para assegurar a adequação e eficácia do sistema de gestão da qualidade;

(f) Uma declaração escrita em como o mesmo pedido não foi apresentado a nenhum outro organismo notificado.

3.2. O sistema de gestão da qualidade é avaliado pelo organismo notificado, que determina se esse sistema cumpre os requisitos referidos no artigo 17.º.

A decisão é notificada ao fornecedor ou ao seu mandatário.

A notificação inclui as conclusões da avaliação do sistema de gestão da qualidade e a decisão de avaliação fundamentada.

3.3. O fornecedor deve continuar a aplicar e a manter o sistema de gestão da qualidade aprovado de maneira que este permaneça adequado e eficiente.

3.4. O fornecedor deve comunicar ao organismo notificado qualquer alteração planeada do sistema de gestão da qualidade aprovado ou da lista de sistemas de IA abrangidos por este último.

As alterações propostas são analisadas pelo organismo notificado, a quem cabe decidir se o sistema de gestão da qualidade alterado continua a satisfazer os requisitos enunciados no ponto 3.2 ou se será necessário proceder a nova avaliação.

O organismo notificado notifica o fornecedor da sua decisão. A notificação inclui as conclusões da análise das alterações e a decisão de avaliação fundamentada.

4. Controlo da documentação técnica.

4.1. Além do pedido referido no ponto 3, o fornecedor deve apresentar junto do organismo notificado da sua escolha um pedido de avaliação da documentação técnica relativa ao sistema de IA que o fornecedor tenciona colocar no mercado ou colocar em serviço e que seja abrangido pelo sistema de gestão da qualidade referido no ponto 3.

4.2. O pedido deve incluir:

(a) O nome e o endereço do fornecedor;

(b) Uma declaração escrita em como o mesmo pedido não foi apresentado a nenhum outro organismo notificado;

(c) A documentação técnica referida no anexo IV.

4.3. O organismo notificado analisa a documentação técnica. Sempre que pertinente e limitado ao necessário para o desempenho das suas funções, deve ser concedido ao organismo notificado total acesso aos conjuntos de dados de treino, validação e testagem utilizados, inclusive, se for caso disso e sob reserva de salvaguardas de segurança, através de interfaces de programação de aplicações ou outros meios e ferramentas técnicas pertinentes que possibilitem o acesso remoto.

4.4. Ao analisar a documentação técnica, o organismo notificado pode requerer que o fornecedor apresente mais provas ou realize mais testes de maneira que permita uma adequada avaliação da conformidade do sistema de IA com os requisitos estabelecidos no título III, capítulo 2. Se o organismo notificado não ficar satisfeito com os testes realizados pelo fornecedor, deve realizar diretamente os testes adequados que sejam necessários.

4.5. Deve ser concedido aos organismos notificados o acesso ao código-fonte do sistema de IA mediante pedido fundamentado e apenas se estiverem preenchidas cumulativamente as seguintes condições:

a) O acesso ao código-fonte é necessário para avaliar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no título III, capítulo 2, e

b) Os procedimentos de testagem/auditoria e as verificações baseadas nos dados e na documentação apresentados pelo fornecedor foram esgotados ou revelaram-se insuficientes.

4.6. A decisão é notificada ao fornecedor ou ao seu mandatário. A notificação inclui as conclusões da avaliação da documentação técnica e a decisão de avaliação fundamentada.

Se o sistema de IA estiver em conformidade com os requisitos estabelecidos no título III, capítulo 2, o organismo notificado emite um certificado UE de avaliação da documentação técnica. Esse certificado deve indicar o nome e o endereço do fornecedor, as conclusões do exame, as (eventuais) condições da sua validade e os dados necessários à identificação do sistema de IA.

O certificado e os seus anexos devem conter todas as informações necessárias para permitir a avaliação da conformidade do sistema de IA e o controlo do sistema de IA durante a utilização, se for caso disso.

Se o sistema de IA não estiver em conformidade com os requisitos estabelecidos no título III, capítulo 2, o organismo notificado recusa a emissão de um certificado UE de avaliação da documentação técnica e informa o requerente do facto, fundamentando pormenorizadamente as razões da sua recusa.

Se o sistema de IA não cumprir o requisito relativo aos dados utilizados para o treinar, será necessário voltar a treinar o sistema de IA antes da apresentação do pedido de nova avaliação da conformidade. Nesse caso, a decisão de avaliação fundamentada pela qual o organismo notificado recusa a emissão do certificado UE de avaliação da documentação técnica inclui considerações específicas sobre a qualidade dos dados utilizados para treinar o sistema de IA, designadamente as razões da não conformidade.

4.7. Qualquer alteração do sistema de IA que possa afetar a conformidade do sistema de IA com os requisitos ou com a finalidade prevista deve ser aprovada pelo organismo notificado que emitiu o certificado UE de avaliação da documentação técnica. O fornecedor informa o referido organismo notificado se tencionar introduzir alterações como as supramencionadas ou se, de algum outro modo, tiver conhecimento da ocorrência dessas alterações. As alterações planeadas são examinadas pelo organismo notificado, a quem cabe decidir se estas exigem que se proceda a uma nova avaliação da conformidade nos termos do artigo 43.º, n.º 4, ou se a situação pode ser resolvida com um aditamento ao certificado UE de avaliação da documentação técnica. Neste último caso, o organismo notificado examina as alterações, notifica o fornecedor da sua decisão e, se as alterações forem aprovadas, emite ao fornecedor um aditamento ao certificado UE de avaliação da documentação técnica.

5. Fiscalização do sistema de gestão da qualidade aprovado.

5.1. O objetivo da fiscalização realizada pelo organismo notificado a que se refere o ponto 3 é garantir que o fornecedor cumpre fielmente os termos e as condições do sistema de gestão da qualidade aprovado.

5.2. Para efeitos de avaliação, o fornecedor deve autorizar o organismo notificado a aceder às instalações onde decorre a conceção, o desenvolvimento e a testagem dos sistemas de IA. O fornecedor deve igualmente partilhar com o organismo notificado todas as informações necessárias.

5.3. O organismo notificado efetua auditorias periódicas para se certificar de que o fornecedor mantém e aplica o sistema de gestão da qualidade e faculta ao fornecedor um relatório de auditoria. No contexto das referidas auditorias, o organismo notificado pode realizar testes adicionais aos sistemas de IA em relação aos quais foi emitido um certificado UE de avaliação da documentação técnica.

ANEXO VIII

INFORMAÇÕES A APRESENTAR AQUANDO DO REGISTO DE OPERADORES E SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO NOS TERMOS DO ARTIGO 51.º

Os fornecedores, os mandatários e os utilizadores que sejam autoridades, agências ou organismos públicos devem apresentar as informações referidas na parte I. Os fornecedores ou, se for caso disso, os mandatários devem assegurar que as informações sobre os seus sistemas de IA de risco elevado a que se refere a parte II, pontos 1 a 11, são completas, corretas e atualizadas. As informações referidas no ponto II.12 serão geradas automaticamente pela base de dados.

Parte I. Informações relativas aos operadores (após o registo dos operadores)

-1. Tipo de operador (fornecedor, mandatário ou utilizador);

1. Nome, endereço e contactos do fornecedor;

2. Se as informações forem apresentadas por outra pessoa em nome do operador, nome, endereço e contactos dessa pessoa;

Parte II. Informações relativas ao sistema de IA de risco elevado

1. Nome, endereço e contactos do fornecedor;

2. Nome, endereço e contactos do mandatário, se for caso disso;

3. Designação comercial do sistema de IA e quaisquer outras referências inequívocas que permitam identificar e rastrear o sistema de IA;

4. Descrição da finalidade prevista do sistema de IA;

5. Estado do sistema de IA (no mercado ou em serviço; já não se encontra no mercado/em serviço; retirado);

6. Tipo, número e data de validade do certificado emitido pelo organismo notificado e o nome ou número de identificação desse organismo notificado, quando aplicável;

7. Uma cópia digitalizada do certificado referido no ponto 6, quando aplicável;

8. Os Estados-Membros onde o sistema de IA está ou foi colocado no mercado ou colocado em serviço ou disponibilizado na União;

9. Uma cópia da declaração de conformidade UE referida no artigo 48.º;

10. Instruções de utilização em formato eletrónico;

11. URL para informações adicionais (opcional).

12. Nome, endereço e contactos dos utilizadores;

ANEXO VIII-A

INFORMAÇÕES A APRESENTAR AQUANDO DO REGISTO DOS SISTEMAS DE IA DE RISCO ELEVADO ENUMERADOS NO ANEXO III EM RELAÇÃO À TESTAGEM EM CONDIÇÕES REAIS EM CONFORMIDADE COM O ARTIGO 54.º-A

As informações a seguir indicadas devem ser fornecidas e, subsequentemente, mantidas atualizadas no respeitante à testagem em condições reais a efetuar em conformidade com o artigo 54.º-A:

1. Número único de identificação a nível da União da testagem em condições reais;

2. Nome e contactos do fornecedor ou potencial fornecedor e dos utilizadores envolvidos na testagem em condições reais;

3. Uma breve descrição do sistema de IA, da sua finalidade prevista e outras informações necessárias para a identificação do sistema;

4. Um resumo das principais características do plano de testagem em condições reais;

5. Informações sobre a suspensão ou cessação da testagem em condições reais;

ANEXO IX

LEGISLAÇÃO DA UNIÃO RELATIVA A SISTEMAS INFORMÁTICOS DE GRANDE ESCALA NO ESPAÇO DE LIBERDADE, SEGURANÇA E JUSTIÇA

1. Sistema de Informação de Schengen

   (a) Regulamento (UE) 2018/1860 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo à utilização do Sistema de Informação de Schengen para efeitos de regresso dos nacionais de países terceiros em situação irregular (JO L 312 de 7.12.2018, p. 1).

   (b) Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira, e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006 (JO L 312 de 7.12.2018, p. 14).

   (c) Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

2. Sistema de Informação sobre Vistos

   (a) Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que altera o Regulamento (CE) n.º 767/2008, o Regulamento (CE) n.º 810/2009, o Regulamento (UE) 2017/2226, o Regulamento (UE) 2016/399, o Regulamento XX/2018 [Regulamento Interoperabilidade] e a Decisão 2004/512/CE e que revoga a Decisão 2008/633/JAI do Conselho [COM(2018) 302 final]. A atualizar assim que os colegisladores adotarem o Regulamento (abril/maio de 2021).

3. Eurodac

(a) Proposta alterada de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à criação do sistema "Eurodac" de comparação de dados biométricos para efeitos da aplicação efetiva do Regulamento (UE) XXX/XXX [Regulamento Gestão do Asilo e da Migração] e do Regulamento (UE) XXX/XXX [Regulamento Reinstalação], da identificação de nacionais de países terceiros ou apátridas em situação irregular, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera os Regulamentos (UE) 2018/1240 e (UE) 2019/818 [COM(2020) 614 final].

4. Sistema de Entrada/Saída

(a) Regulamento (UE) 2017/2226 do Parlamento Europeu e do Conselho, de 30 de novembro de 2017, que estabelece o Sistema de Entrada/Saída (SES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros, que determina as condições de acesso ao SES para efeitos de aplicação da lei, e que altera a Convenção de Aplicação do Acordo de Schengen e os Regulamentos (CE) n.º 767/2008 e (UE) n.º 1077/2011 (JO L 327 de 9.12.2017, p. 20).

5. Sistema Europeu de Informação e Autorização de Viagem

(a) Regulamento (UE) 2018/1240 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que cria um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e altera os Regulamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (JO L 236 de 19.9.2018, p. 1).

(b) Regulamento (UE) 2018/1241 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que altera o Regulamento (UE) 2016/794 para efeitos da criação de um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) (JO L 236 de 19.9.2018, p. 72).

6. Sistema Europeu de Informação sobre Registos Criminais de nacionais de países terceiros e de apátridas

(a) Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN) tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e que altera o Regulamento (UE) 2018/1726 (JO L 135 de 22.5.2019, p. 1).

7. Interoperabilidade

(a) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos (JO L 135 de 22.5.2019, p. 27).

(b) Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração (JO L 135 de 22.5.2019, p. 85).